NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

RISK OF CYBERTERRORISM TO NAVAL SHIPS INPORT NAVAL STATION EVERETT: A MODEL BASED PROJECT UTILIZING SIAM

by

Rodrick “Rick” A. Tester

March 2007

Thesis Advisor:	Dorothy Denning
Second Reader:	Steve Iatrou

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Risk of Cyber Attack to Naval Ships Inport Naval Station Everett: A Model Based Project Utilizing SIAM

5. FUNDING NUMBERS

6. AUTHOR(S) LT Rodrick A. Tester, USN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

Based on numerous high level concerns that the cyber threat is expected to increase, as well as the already documented uses of cyber warfare, it is necessary to ensure our naval ships are hardened against such attacks. In doing so, an influence net model was designed to discover the likelihood of a successful cyber attack. However, first it was necessary to establish what the best mitigation tools are in defense of cyber attack methods. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security. In combination with the expert opinion surveys and in looking at research and established security techniques it should become apparent whether or not ships are taking all the required steps to best secure themselves against an attack.

Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States and the risk for each particular U.S. asset can be evaluated. Additionally, this tool can also facilitate security funding as well as establishing a means of prioritizing the tools for protection if the network needs to be hastily re-established after an attack. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.

14. SUBJECT TERMS
Cyberterrorism, information assurance, computer security, influence net model, Situational Influence Assessment Module (SIAM)

15. NUMBER OF PAGES
95

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

RISK OF CYBER ATTACK TO NAVAL SHIPS INPORT NAVAL STATION EVERETT: A MODEL BASED PROJECT UTILIZING SIAM

Rodrick A. Tester
Lieutenant, United States Navy
B.A., University of Minnesota, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Author: LT Rodrick A. Tester, U.S. Navy

Approved by: Dr. Dorothy Denning
Thesis Advisor

Mr. Steven Iatrou
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Based on numerous high level concerns that the cyber threat is expected to increase, as well as the already documented uses of cyber warfare, it is necessary to ensure our naval ships are hardened against such attacks. In doing so, an influence net model was designed to discover the likelihood of a successful cyber attack. However, first it was necessary to establish what the best mitigation tools are in defense of cyber attack methods. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security. In combination with the expert opinion surveys and in looking at research and established security techniques it should become apparent whether or not ships are taking all the required steps to best secure themselves against an attack.

Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States and the risk for each particular U.S. asset can be evaluated. Additionally, this tool can also facilitate security funding as well as establishing a means of prioritizing the tools for protection if the network needs to be hastily re-established after an attack. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I would like to thank my thesis advisor, Dr. Dorothy Denning for her impeccable advice and guidance throughout this project. Her superb knowledge in the field and her patience with my inadequacies made this tedious process actually enjoyable. I would also like to thank Mr. Steve Iatrou, my second reader, whom on numerous occasions helped relieve me of my thesis anxieties and always lead me down the right path. His golfing counsel isn't bad either. I would also like to thank all the individuals whom filled out and returned the expert opinion surveys; Professors, Karen Burke, Paul Clark, Daniel Warren and ITCS(SW/AW) Billy Freeman from the Bureau of Naval Personnel. Special thanks must go out to my good friend Ian Brown, for all of his assistance throughout my stay in the Monterey Area and especially for the vital assistance he graciously provided during the last few weeks of my thesis.

I would also like to thank my wonderful bride Heather, who while working on her own degree at California State University Monterey Bay managed to support me and share tasks to ensure our goals were met. Additionally, I would like to thank my three daughters; Sabrina, Victoria, and Selena for their understanding during crunch times both during finals and throughout this thesis process. Their love and tremendous support were an encouragement and greatly lead to my successful completion of Master's of Science in Information Systems and Operations.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION BEHIND THE RESEARCH

As stated by the founder of the term “Cyber War,” Dr. John Arquilla, in a PBS FRONTLINE interview referring to Operation Iraqi Freedom, “It occurred to me, in the wake of that tremendous and lopsided victory of ours, that much of what we did could have been held hostage to the disruption of any of those information systems. That was the beginning of cyber war – the idea that the vulnerability of communications could cripple an advanced army. What makes it strong also made it weak.” The military acknowledges this frightful fact and understands the increasingly indispensable nature of information technology, as well as how this indispensable technology has transformed these systems into high value targets of cyber terrorists, which presents a significant threat to both the military and national security.

In a study by Charles Billo and Welton Chang, Senior Research Associate and Research Intern, respectively, for the Institute for Security Technology Studies at Dartmouth College, <u>Cyber Warfare; An Analysis of the Means and Motivations of Selected Nation States</u> (2004), noted “cyber warfare” as warfare that involves,

> ...units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks are the primary executors of these attacks. These individuals often operate under auspices and possible support of nation-state actors. In the future, if not already common practice, individual cyber warfare units will execute attacks against targets in a cooperative and simultaneous manner.

Information Operations Issue Manager for the CIA, John Serbian, in a Statement for the Record before the Joint Economics Committee, U.S. Congress on 23 February 2000, paints a vivid picture. Serbian states that for adversaries who cannot match US strength, the use of asymmetric strategies to exploit vulnerabilities will continue to have incentives. The incentives cyber attacks provide as stated by Serbian include economic, industrial, and military rationales. By way of example:

"Trillions of dollars in financial transactions and commerce move over a medium with minimal protection and only sporadic law enforcement - a structure the most complex the world has ever known. Increasing quantities of intellectual property reside on networked systems; and opportunities abound to disrupt military effectiveness and public safety while maintaining the elements of surprise and anonymity" (Serbian, 2000).

John Serbian continues in his explanation of the "threat" to Congress, that the information infrastructure that was built is interoperable, easy to access, and easy to use. Also, with attributes like openness and ease of connectivity are the same ones that now make the systems vulnerable to attacks against automated information systems. He further explains that the cyber threat can "originate from any location, affect systems anywhere in the world, disguise origins and travel routes, and do it instantaneously." Further, Serbian explains how being a part of the "cyber attack game" does not take a great deal of skill or investment and explains that cyber tools are readily available on the internet for anyone to download and use maliciously. Some tools, he states, even use a point-and-click feature to start an attack (Serbian, 2000).

Serbian also refers to a testimony before the Senate Select Committee on Intelligence by Director of Central Intelligence George Tenet in February of 2000. In DCI Tenet's testimony he stated that the, "foreign cyber threat is one of the key transnational issues that we face as a nation." Also in that testimony, Director Tenet noted that the US is increasingly dependent on "…the unimpeded and secure flow of technology" and that "any adversary that could develop the ability to interrupt that flow…will have the potential to weaken us dramatically or even render us helpless" (Serbian, 2000).

Cyber warfare has already been used as a tool of military warfare against this country, as addressed by Dr. Dorothy Denning, Professor of Defense Analysis at the Naval Postgraduate School in Monterey California and former Professor of Computer Science at Georgetown University. In her book, Information Warfare and Security she explains how the US military encountered Netherland hackers during the first Gulf War. The hackers were able to penetrate 34 American military internet sites, gathering information on military supply systems, troop locations and their weapons, as well as US

Navy ship movements and the capabilities of the Army’s Patriot Missile (Denning, 1999). Had the Iraqi government suspicions of a trap not prevented them from purchasing this data, the length of the war perhaps may have been longer, though it is unlikely the information stolen would have actually changed the outcome of the war. However, this does give a general idea of the possibilities and potential use of cyber warfare in the future.

It was the aforementioned CIA statements concerning cyber threats and their expected increased use, coupled with the already documented uses of cyber warfare addressed by Dr. Denning, that has spawned this research.

B. GENERAL SCOPE OF THE THESIS

The main thrust of this study will be the design of a model which will help to discover whether ships are hard targets, targets of opportunity, targets of choice, or simply soft targets. Looking at research and established security techniques it will become apparent whether or not ships are taking all the required steps to best secure themselves against an attack.

Though the “insider” may be the biggest threat to an organization (Denning, 1999) for the purposes of this study the focus will be on the “outsider” hacker/terrorist. To prevent this research from becoming classified, only theoretical data are presented concerning what may be considered a typical ship in the Everett, WA region. Some of the past terrorist information and threats addressed in making the model are also theoretical unless noted otherwise. In such cases the information was taken only from open source materials such as the internet or unclassified research.

C. BRIEF EXPLANATION OF METHODOLOGY

This thesis will focus on identifying the likelihood of a successful cyber attack on an Everett based ship. In order to do so, an expert opinion survey was designed and completed by individuals currently working in the field of network security, to determine expected levels of protection each mitigation tool provides against known cyberterrorist attack methods. Once the expert opinion analysis was completed it was built into an influence net model, along with cyber terrorist motivations and means to determine whether or not a cyberterrorist attack is likely to succeed against a U.S. ship.

Additionally, the model was tested using various boundary case scenarios to evaluate usability, completeness, and accuracy. The model allows many scenarios (or case studies) to be considered in order to produce the optimal outcome for Navy ships. A worst case scenario can also be analyzed to show how much more likely the ship will be at risk not having a particular security mechanism in place.

D. BENEFITS OF STUDY

The benefits of the study are numerous. First, the expert opinion survey data alone will prove vital in determining the best security practices available to counter individual attack methods. Additionally, the work will strive to determine the amount of risk navy ships are in, as well as determining what they can do to mitigate the risk of becoming targets of opportunity. Such information will assist in protecting ships from attack by giving decision makers the ability to see the main vulnerabilities of a typical ship's computer networks, as well as how important certain mitigation tools are toward the defense of a network. The use of the completed model can also facilitate security funding as well as establishing a means of prioritizing the security mechanisms for protection if a network needs to be hastily re-established after an attack.

Though the initial model was designed around a theoretical Naval Station Everett ship, with modification the model can be utilized for any naval asset throughout the United States, and the risk for each particular U.S. asset can be evaluated. Ultimately, the protection of a ship's computer networks against cyber terrorist threats is fundamental in ensuring continued effective command and control and ultimately the security of this nation.

E. THESIS STRUCTURE:

Chapter I – Introduction – This chapter provides the thesis statement and describes the general scope of the thesis. It gives an overview of the chapters, figures and annexes of the paper.

Chapter II - Background Information – This chapter describes many of the general Information Operations' terms and key concepts. Additionally, it explores the motivations of hackers and cyberterrorists as well as the expected tools used by these criminals. The chapter concludes by addressing the protection mechanisms used to protect against terrorists (i.e., the DITSCAP process as well as individual mitigation tools).

Chapter III - Situational Influence Assessment Module - This chapter introduces influence net modeling and the SIAM program.

Chapter IV – Model Set-up – This chapter describes how the model for this thesis was designed, including node breakdown and link strength assignments.

Chapter V - Model Demonstration and Results – This chapter describes the results of the model.

Chapter VI - Future Work & Conclusion – This chapter looks at areas of potential further research, and gives a brief summary of the work accomplished by this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND INFORMATION

> The United States of America is fighting a war against terrorists of global reach. The enemy is not a single political regime or person or religion or ideology. The enemy is terrorism—premeditated, politically motivated violence perpetrated against innocents.
>
> -The National Security Strategy of the United States of America, September 2002

A. INTRODUCTION TO INFORMATION OPERATIONS

Joint Publication 3-13, titled, Information Operations of 13 February 2006 is the joint doctrine for U.S. military conducting Information Operations (IO). It provides the guidance to help prepare, plan, execute, and assess IO in support of joint military operations. Information Operations is described by Pub 3-13 as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

In support of this thesis we will look only at Computer Network Operations. CNO is the newest of the core capabilities and consists of Computer Network Attack (CNA), Computer Network Defense (CND), which will be the focus of this paper, and the related computer network exploitation (CNE). In this day and age of technology, CNO capabilities are ever increasing, in parallel with the increasing numbers of networked computers and supporting IT infrastructure systems. CNO is primarily used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure and thus is the IO capability best designed to exploit the new opportunities and vulnerabilities of our adversaries as well as protecting our own. (JP 3-13, 2006)

Specifically, CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense (DoD) information systems and computer networks. CND actions not only protect DoD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations.

CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

As the capability of computers and the range of their employment broaden, new vulnerabilities and opportunities will continue to develop. This offers both opportunities to attack and exploit an adversary's computer system weaknesses and a requirement to identify and protect our own from similar attack or exploitation. Therefore, with the broad definitions of IO described above it is practical to explain the means in which we measure and protect these systems.

B. INFORMATION ASSURANCE

Per DoD Directive 8500.1 (2002): Information Assurance is defined as: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. The Committee on National Security Systems (CNSS) defines these key terms in their National Information Assurance (IA) Glossary:

1. Availability

Timely, reliable access to data and information services for authorized users

2. Integrity

Condition existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.

3. Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or means of verifying an individual's authorization to receive specific categories of information.

4. Confidentiality

Assurance that information is not disclosed to unauthorized persons, processes, or devices.

5. Non-repudiation

Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of sender's identity, so neither can later deny having processed the data.

With key information assurance terms defined we will now look at those that threaten information systems as well as their motives.

C. CYBER THREATS AND THEIR MOTIVES

Dr. Denning in her book Information Warfare and Security (1999) addresses many of the offensive actors of information warfare. These groups consist of insiders, hackers, criminals, corporations, and terrorists, any of which may use information systems to conduct intelligence gathering, conduct financial gain endeavors or disruption operations (i.e., block legitimate access to information) or, simply as a means of thrill seeking. Though, this thesis is primarily concerned with hackers, criminals and cyber terrorists, all of the aforementioned groups from Dr. Denning's book will be briefly explained along with their principle motivations.

1. Insiders

This category consists of trusted individuals with inside access (i.e., employees and contractors) to a particular organization's information resources. Insiders may act as salesmen of corporate information, selling the information to organized crime syndicates, foreign governments, and/or competitors. Aside from exploiting information, certain disgruntled insiders may use their inside access to destroy their employers information and information resources.

2. Hackers

This group of offensive players typically consists of those that "gain access to or break into electronic systems, particularly computers and telecommunications equipment." Motivations behind hacking can be numerous including thrills, challenge, power and financial gain. Regardless of a hacker's motive; their actions damage the integrity of systems and can be a major nuisance (Denning, 1999).

3. Criminals

This category of threat targets financial information resources, and as expected are motivated by money. Criminals look for information such as credit card numbers, bank account information and basically anything that can be converted to, or sold for cash. Criminals also utilize internet and other information resources to engage in any number of internet scams and frauds.

4. Corporations

Corporations are also motivated by money, as well as competitive position. They actively seek intelligence from their competitors, such as trade secrets and frequently rely on the aforementioned "insider" for such information.

5. Government Agencies

This category consists of law enforcement and intelligence agencies motivated to protect public safety and national security. Dr. Denning describes an example use by law enforcement as they target a criminal's communications and other structures for gathering evidence in support of criminal cases, whereas, intelligence agencies seek "military, diplomatic, and economic secrets of foreign governments, foreign corporations, and foreign adversaries" in support of our nation's goals of national security (Denning, 1999).

6. Terrorists

Though cyber terrorists have yet to make any major appearances, they are considered to be of particular interest because of their potential to do damage. In promoting their cause, terrorists may conduct intelligence gathering to collect information about their targets, spread propaganda and conduct attacks "against critical infrastructures such as emergency services and financial systems." Terrorists may also utilize the Internet in the same manner as the aforementioned criminals in order to earn funds to support there next mission.

The various groups above have various motivations for their actions, however, for this thesis we will focus on four main categories, which are, "financial gain," "intelligence gathering," "disruption of operations," and lastly, "thrill seeking." Insiders, criminals, and corporations are mainly motivated by financial gain, however, a personal vendetta could also cause an employee to divulge insider information or commit sabotage against his organization. Hackers, on the other hand, though sometimes motivated by money, are more motivated by thrills, challenge, and power as addressed by Dr. Denning.

With the various actors described, this thesis will now attempt to describe how the aforementioned actors accomplish their objectives.

D. VULNERABILITIES

Cyber criminals attack an information system via its vulnerabilities, which the CNSS Glossary defines as, "a weakness in an information system (IS), or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited" (CNSS, 2007). A key point about IS vulnerabilities is that they are similar for everyone and can be exploited by anyone via an Internet connection. Additionally, information about IS vulnerabilities and tools that exploit them are publicly available for anyone interested enough to look using any Internet search engine. Navy IS's are just as vulnerable as other systems and just as susceptible to exploitation if they are not properly protected.

SANS Institute[1] publishes what they consider to be the 20 most critical vulnerabilities of information systems. These critical vulnerabilities include versions of Microsoft Windows, MAC OS X and UNIX operating system vulnerabilities, as well as vulnerabilities with cross-platform applications such as databases, and web applications (e.g., Content Management Systems (CMS), wikis, portals, bulletin boards, and discussion forums). Another critical vulnerability SANS addresses is with the Microsoft Internet Explorer browser, which is installed by default with Microsoft operating systems. This browser has numerous vulnerabilities that if not patched can allow an attacker to corrupt memory, conduct spoofing and even execute arbitrary scripts (SANS, 2007).

Another category of vulnerabilities listed by SANs is "network devices" which incorporates vulnerabilities with "various products such as Cisco Unified Call Manager, Asterisk and a number of VoIP phones from various vendors." These particular network devices were discovered to contain vulnerabilities that can either lead to a crash or cause

[1] SANS Institute (SysAdmin, Audit, Networking, and Security) is a trade name owned by the for-profit Escal Institute of Advanced Technologies. SANS provides computer security training, professional certification, and a research archive. It was founded in 1989.

a complete control over the vulnerable server/device. By gaining control over the VoIP server and phones, an attacker could carry out VoIP phishing scams, eavesdropping, toll fraud or denial-of-service attacks. (SANS, 2007)

E. TOOLS OF THE CYBER CRIMINALS

Cyber criminals have a myriad of tools to choose from in an attempt to accomplish their objectives. The following list of tools was derived from the US Army's Training Handbook, "A Military Guide to Terrorism in the Twenty-First Century" (2004). This list is not all inclusive but is a very good starting point.

1. Backdoor

Hidden software or hardware mechanism used to circumvent security controls. A backdoor is synonymous with trapdoor.

2. Denial of Service (DOS) Attack

An attack designed to disrupt network service, typically by overwhelming the system with millions of requests every second causing the network to slow down or crash.

3. Distributed Denial of Service (DDOS) Attack

A denial of service attack that involves the use of numerous computers to simultaneously flood the target.

4. E-mail Spoofing

A method of sending e-mail to a user that appears to have originated from one source when it actually was sent from another source. This method is often an attempt to trick the user into releasing sensitive information (such as passwords).

5. IP Address Spoofing

A method that creates Internet Protocol (IP) packets using somebody else's IP address. Routers use the destination IP address to forward packets through the Internet, but ignore the source IP address. This method is often used in DDOS attacks in order to hide the true identity of the attacker.

6. Key Logger

A software program or hardware device that is used to monitor and log each of the keys a user types on a computer keyboard. The adversary who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the actual keys being typed, the adversary can easily obtain passwords and other information the computer operator may not wish others to know. Key loggers are a type of spyware, which are detailed below.

7. Logic Bomb

A software program with malicious code that lies dormant until some event occurs, at which point it executes to destroy data on a computer. If execution is triggered by a date or time, as is often the case, the program is also called a "time bomb" (Denning, 1999).

8. Packet Sniffing

A program and/or device that monitors data traveling over a network. Although sniffers are used for legitimate network management functions, they also are used during cyber attacks for stealing information, including passwords, off a network. Once emplaced, they are very difficult to detect and can be inserted almost anywhere.

9. Spoofing

Attempt to gain access to an information system by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.

10. Spyware

Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is software that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program.

11. Trojan Horse

A program or utility that falsely appears to be a useful program or utility such as a screen saver. However, once installed, it performs a function in the background such as allowing other users to have access to your computer. The users can then send information from your computer to other computers, or allow unauthorized collection, falsification, or destruction of information.

12. Viruses

A malicious software program, script, or macro that has been designed to infect, destroy, modify, or cause other problems with a computer or software program. Viruses replicate and attach themselves to a host, (e.g., files) with no obvious signs of its presence. There are many different types of viruses, a few examples include: boot sector virus, companion virus, executable virus, overwrite virus, polymorphic virus, resident and stealth viruses.

13. Worms

A destructive software program containing code capable of gaining access to networked computers and, once within a computer, causing that computer harm, for example, by deleting, modifying, distributing, or otherwise manipulating the data. Worms can replicate from machine to machine across network connections, often clogging networks and computer systems as it spreads.

14. Zombie

A computer or server that has been basically hijacked using some form of malicious software to help a hacker perform a Distributed Denial of Service attack (DDOS) or send out spam.

With the tools of cyber criminals and other background information explained above, this thesis will now describe SIAM modeling as well as give a basic model to give the reader a foundation for SIAM’s use in later chapters.

III. SITUATIONAL INFLUENCE ASSESSMENT MODULE (SIAM)

A. SIAM DESCRIBED

The SIAM software application is a collaborative decision support tool, designed to assist people in analyzing complex problems and issues by breaking them down into smaller more workable parts. The smaller parts allow the modeler to more easily recognize and evaluate critical relationships among the varying parts, as well as determine the importance each particular part plays in the larger scheme (Rosen and Smith, 2006).

SIAM designers, Dr. Julie Rosen and Mr. Wayne Smith of the Science Applications International Corporation (SAIC), state that their product eases the building and analysis of an Influence Net Model, which they define as “a user-created model that depicts events and their causal interrelationships. It is a graphical model that facilitates brain-storming and complex decision making.” (Influence Nets will be described in greater detail later.) Dr. Rosen and Mr. Smith further state that SIAM is a time saving tool which helps users in examining complex problems by use of the various capabilities it provides, for example:

1. “A graphical model that depicts complex, possibly conflicting, cause-and –effect relationships in an easy-to-manipulate fashion; and

2. Comparative quantitative assessment techniques that evaluate the relative influencing impacts of these accumulated relationships.”

Rosen and Smith also note that with these tools and others, SIAM helps “users organize and evaluate large amounts of information, and collaborate with others in analyzing complex factors and causal dependencies of any given issue” (Rosen and Smith, 2006).

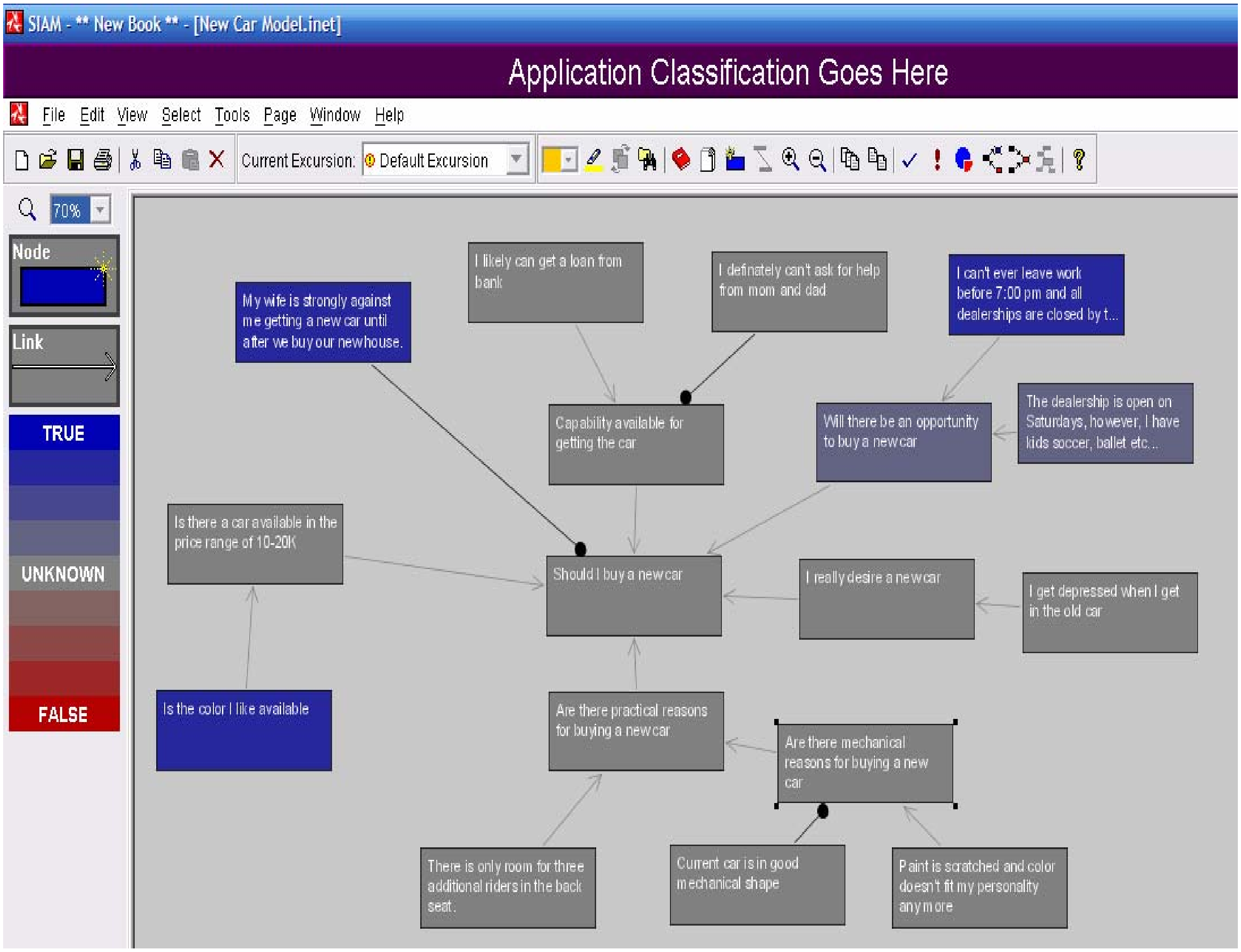
In their description of SIAM, Professors Hayes and Sands of the Naval War College, Center for Naval Warfare Studies, Decision Support Department state “the networks created in SIAM can be used to identify important issues, actions, or factors that can and do influence a specific outcome in a given situation” (Hayes and Sands, 2001).

Rosen and Smith further state that complex problems are typically solved in a group environment (i.e., seminar or workshop) with multiple subject matter experts working toward a similar goal. SIAM can be used in this environment, allowing the seminar group to brainstorm, conduct "what-if" scenarios, and break down issues into their simplest form to be depicted graphically. All the while the group can continually critique and challenge one another's logic and quickly make changes to the model, or simply revise the model as "data changes or experts' opinions change," which can then be reassessed for their impact. Additionally, with the use of SIAM's documentation capabilities, notes can be taken within SIAM to retain the reasoning behind certain decisions and changes, as well as documenting reference material and other pertinent information (Brodhun III 2001, Rosen and Smith 2006).

B. SIAM INFLUENCE NET SAMPLE

An Influence Net is defined as, "A graphical representation of a model, which incorporates perceptions and events the user identifies as important in examining an issue or question. Additionally, an Influence Net is a chain of casual influences that, taken independently, may appear meaningless, but when linked together, establish patterns of behavior and motivating factors in a situation" (Rosen and Smith, 2006).

A simple Influence Net is provided below to show the basic topology of an Influence Net and to help in describing the key elements of the Influence Net model.



SIAM - ** New Book ** - [New Car Model.inet]
Application Classification Goes Here
File Edit View Select Tools Page Window Help
Current Excursion: Default Excursion
70%
Node
Link
TRUE
UNKNOWN
FALSE

My wife is strongly against me getting a new car until after we buy our new house.

I likely can get a loan from bank

I definately can't ask for help from mom and dad

I can't ever leave work before 7:00 pm and all dealerships are closed by t...

Capability available for getting the car

Will there be an opportunity to buy a new car

The dealership is open on Saturdays, however, I have kids soccer, ballet etc...

Is there a car available in the price range of 10-20K

Should I buy a new car

I really desire a new car

I get depressed when I get in the old car

Is the color I like available

Are there practical reasons for buying a new car

Are there mechanical reasons for buying a new car

There is only room for three additional riders in the back seat.

Current car is in good mechanical shape

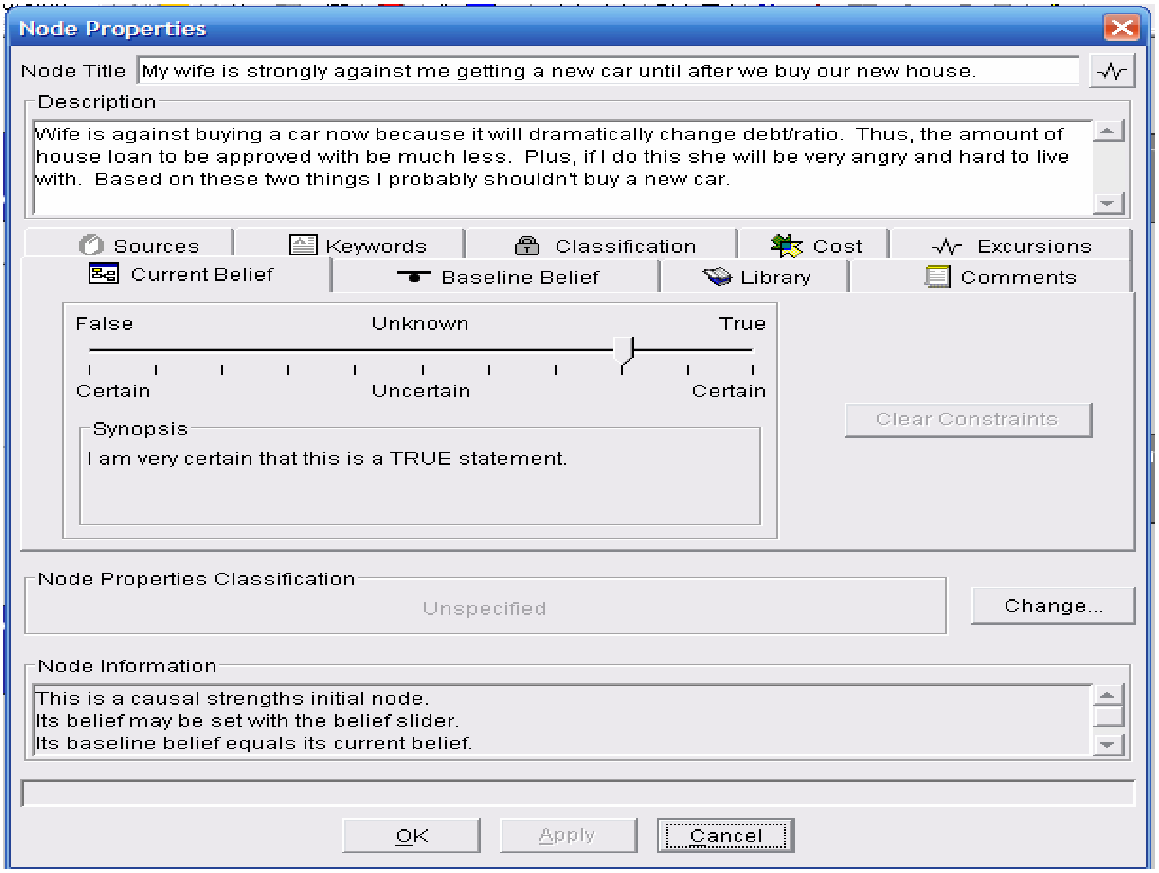
Paint is scratched and color doesn't fit my personality anymore

Figure 1. Basic Influence Net Diagram (of buying a car)

Within the SIAM application, the graphical objects which display the chains of causal influences are called "nodes" and "links." A node "is one of a series of related ideas or events that influence an overreaching issue," and a "link" is the "one-way connection between two nodes" and is graphically depicted as a line.

Nodes within the SIAM model serve various roles: root, parent, child, and initial, and are depicted in the model as colored rectangles. The "root node" is essentially the ultimate conclusion, "or desired end state of the analysis." In Figure 1 the root node is, "Should I buy a new car?" A "parent node," which is also sometimes referred to as the "cause node," is an idea or event that influences other events. A "child node," also sometimes referred to as the "effect node" is an idea or event that results from the parent node. Sometimes a node can be both a parent and a child, when such a case occurs, then the node would be considered a parent when at the source of the link, and a child when at the destination. To reemphasize, child nodes are those that are affected by other nodes and parent nodes are those that affect the outcome. For purposes of the root node above the parent nodes are: opportunity (i.e., Is there a car available?), capability (i.e., Can I afford it?), practicality (i.e., Is there a need?), and desire. The last type of node is the "initial node." They are the originating causal influences, and thus lack parental influences. Basically, initial nodes represent the primary assumptions used to construct the Influence Net.

Each node in the influence chain is assigned a belief value to its occurrence, either by the user for initial nodes, or by SIAMs' Bayesian algorithms for all others. The assignment of "the belief value is based on the conditions specified by its influencing events and relationships in the Influence Net." In looking at Figure 2, we can see for the node, "My wife is strongly…" has been assigned a belief value corresponding to, "I am very certain that this is a true statement by the user." Additionally, you can see how the author added other information deemed pertinent into the "description block" for further reference.



Node Title: My wife is strongly against me getting a new car until after we buy our new house.

Description: Wife is against buying a car now because it will dramatically change debt/ratio. Thus, the amount of house loan to be approved with be much less. Plus, if I do this she will be very angry and hard to live with. Based on these two things I probably shouldn't buy a new car.

Synopsis: I am very certain that this is a TRUE statement.

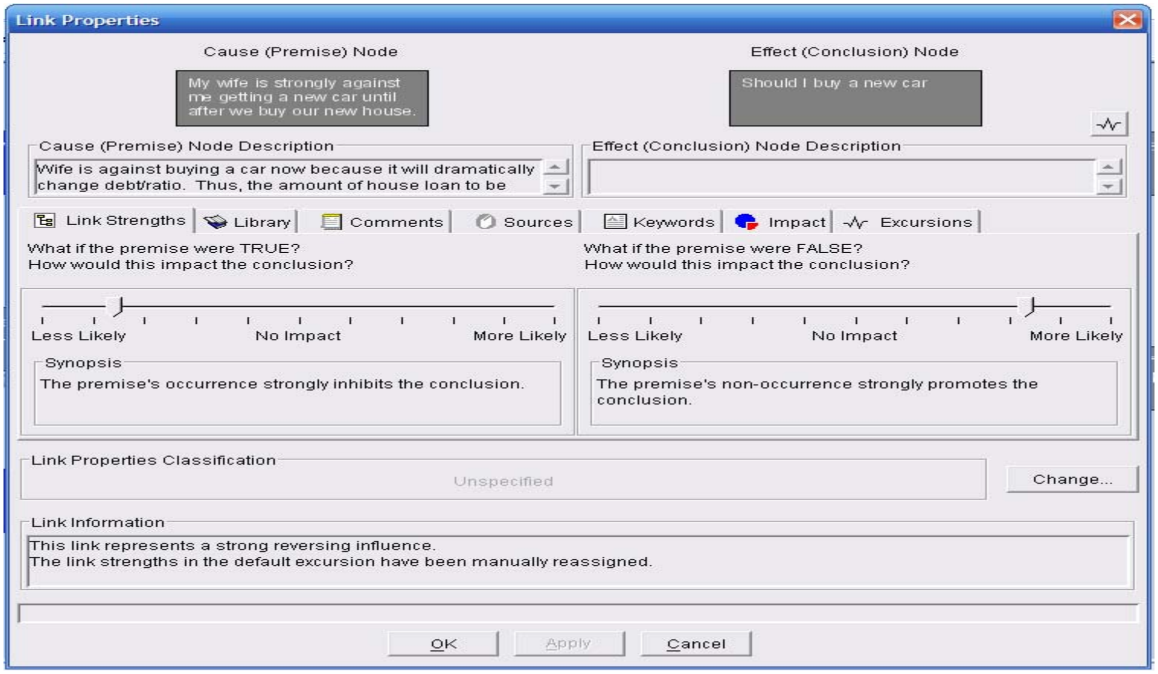
Node Properties Classification: Unspecified

Node Information:
This is a causal strengths initial node.
Its belief may be set with the belief slider.
Its baseline belief equals its current belief.

Figure 2. Node Properties

The belief value, whether assigned by the user or by SIAM, is easily distinguished by a node's color. The color key can be seen on the far left side of Figure 1. The color of a particular node allows the user to quickly identify the relative belief value of that node. "Four shades of blue represent the degrees of uncertainty in the influencing event's truth. Similarly four shades of red depict the degrees of uncertainty that the influencing event is false." If a node color is grey, then this is an indication of complete uncertainty in the likelihood of the influencing event's occurrence. Additionally, for each connecting link there are two link values which must be assigned by the user, one for when the cause (parent) is true and one for when it is not. These link value strengths representing the impact of the cause on the effect, and can be seen in Figure 3 (Rosen and Smith 2006).

By looking back at Figure 1 you will notice the link between the nodes "My wife is strongly…" and "Should I buy a new car" has a filled terminator circle (or ball) at one end of the link. The ball illustrates "that the parent has a reversing influence on the occurrence of the child node," whereas, an arrowhead terminator would indicate "that the parent node has a reinforcing influence on the occurrence of the child node."



Cause (Premise) Node

My wife is strongly against me getting a new car until after we buy our new house.

Effect (Conclusion) Node

Should I buy a new car

Cause (Premise) Node Description

Wife is against buying a car now because it will dramatically change debt/ratio. Thus, the amount of house loan to be

Effect (Conclusion) Node Description

What if the premise were TRUE?
How would this impact the conclusion?

Synopsis
The premise's occurrence strongly inhibits the conclusion.

What if the premise were FALSE?
How would this impact the conclusion?

Synopsis
The premise's non-occurrence strongly promotes the conclusion.

Link Properties Classification
Unspecified

Link Information
This link represents a strong reversing influence.
The link strengths in the default excursion have been manually reassigned.

Figure 3. Link Properties

With a basic SIAM model explained, this thesis will now show how the SIAM software was used to demonstrate a potential cyber attack scenario.

IV. MODEL SET-UP

As previously mentioned the work encompassed in this thesis was designed to model a cyber attack on a US ship, which can also be used to help determine the amount of risk to a particular naval ship. To do so, an Influence Net model was designed around the premise of whether or not a ship can successfully defend against a myriad of cyber attack methods. As Chapter II of this thesis briefly discussed, potential attackers can be motivated by numerous factors, including intelligence gathering, thrill seeking, disrupting operations, and financial gain. Even more importantly, potential attackers have the opportunity, as well as the capability to conduct an attack. The potential of these three key components (i.e., motive, opportunity, and means) coming together could prove disastrous for a Navy ship, or at minimum a nuisance if not properly defended against.

Thousands of attacks occur daily on internet-connected systems. In the first half of 2005 alone, IBM reported that virus-laden emails and criminal driven security attacks increased by 50 percent, with over 237 million overall security attacks. IBM further reported that the US government was the most targeted industry during that period, "with more than 54 million attacks." (IBM, 2005) At that rate it was likely there were over half a billion attacks in 2005, with over 100 million of those attacks being directed toward government systems, including Navy and other DoD systems. In addition to directed attacks, indiscriminate mass attacks such Nimda, Code Red, Slammer, and Blaster, all of which spread rapidly throughout the Internet without sparing vulnerable government computers, are also a considerable threat (Common Sense Guide, 2004). Thus, the threat of attack is real and the need to protect against said attacks requires considerable attention.

The prevalence of attacks and attempted attacks provide evidence of motivation, capability and opportunity, so we will build the model with the assumption that an attack has taken place, as will be demonstrated later in this thesis. Overall, the end goal of network security is to defend against attack – which means defending against each possible type of attack. That being said, the root node, "Ship defends against cyber attack methods" was established, along with the eleven parent nodes, which correspond to the different types of attacks we need to defend against, as illustrated by Figure 4. A summary list is provided:

a. Worm attack aborted

b. Virus attack aborted

c. Trojan Horse penetration aborted

d. Attempt to take over system and turn into Zombie is aborted

e. Denial of Service attack is aborted

f. Keylogger utilization attempt is aborted

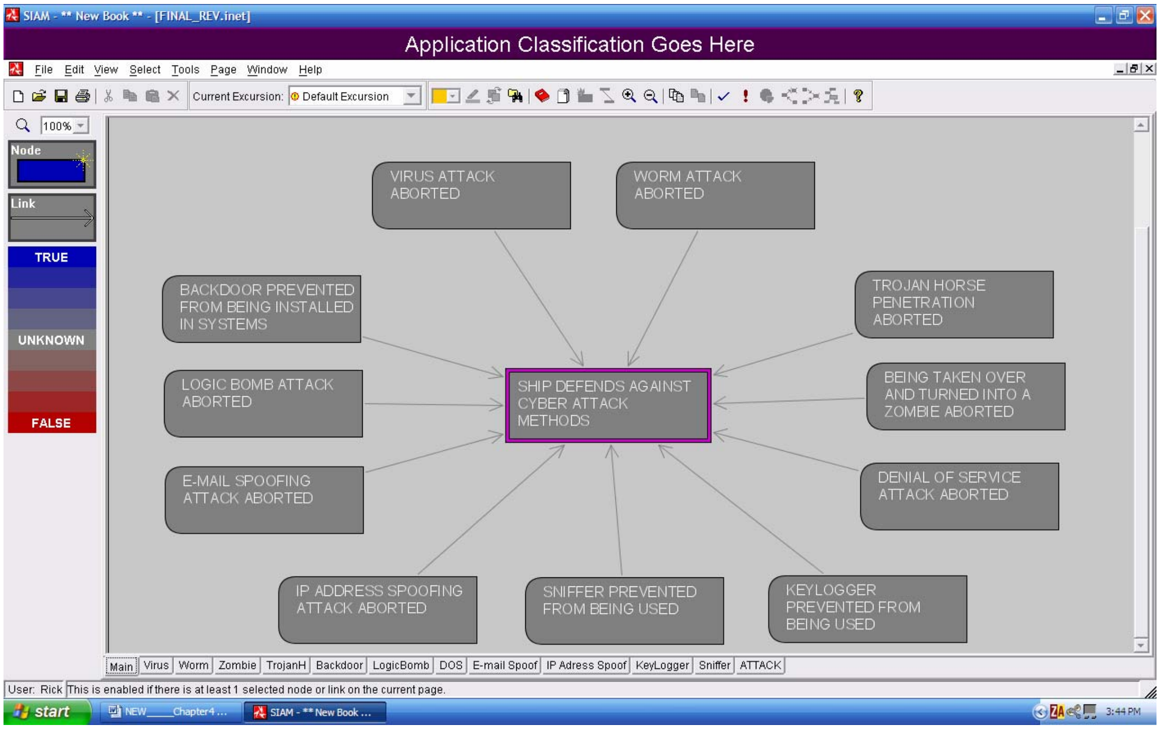
g. Sniffer utilization attempt is aborted

h. IP address Spoofing attack is aborted

i. Email spoofing attack is aborted

j. Backdoor installation attempt is aborted

k. Logic Bomb attack is aborted


SIAM - ** New Book ** - [FINAL_REV.inet]
Application Classification Goes Here
File Edit View Select Tools Page Window Help
Current Excursion: Default Excursion
100%
Node
Link
TRUE
UNKNOWN
FALSE
VIRUS ATTACK ABORTED
WORM ATTACK ABORTED
BACKDOOR PREVENTED FROM BEING INSTALLED IN SYSTEMS
TROJAN HORSE PENETRATION ABORTED
LOGIC BOMB ATTACK ABORTED
SHIP DEFENDS AGAINST CYBER ATTACK METHODS
BEING TAKEN OVER AND TURNED INTO A ZOMBIE ABORTED
E-MAIL SPOOFING ATTACK ABORTED
DENIAL OF SERVICE ATTACK ABORTED
IP ADDRESS SPOOFING ATTACK ABORTED
SNIFFER PREVENTED FROM BEING USED
KEYLOGGER PREVENTED FROM BEING USED
Main Virus Worm Zombie TrojanH Backdoor LogicBomb DOS E-mail Spoof IP Adress Spoof KeyLogger Sniffer ATTACK
start
SIAM - ** New Book ...
3:44 PM

User: Rick This is enabled if there is at least 1 selected node or link on the current page.

Figure 4. Root Node and Parents

After determining the end goal (root node) and the many attack methods (parents) to defend against, it was necessary to consider the likely security measures utilized by U.S. assets and the effect each of these security tools has against the previously mentioned attack methods. Figure 5 illustrates the likely security tools in place to help prevent attacks, which are also listed below.

a. Firewall

b. Hardening

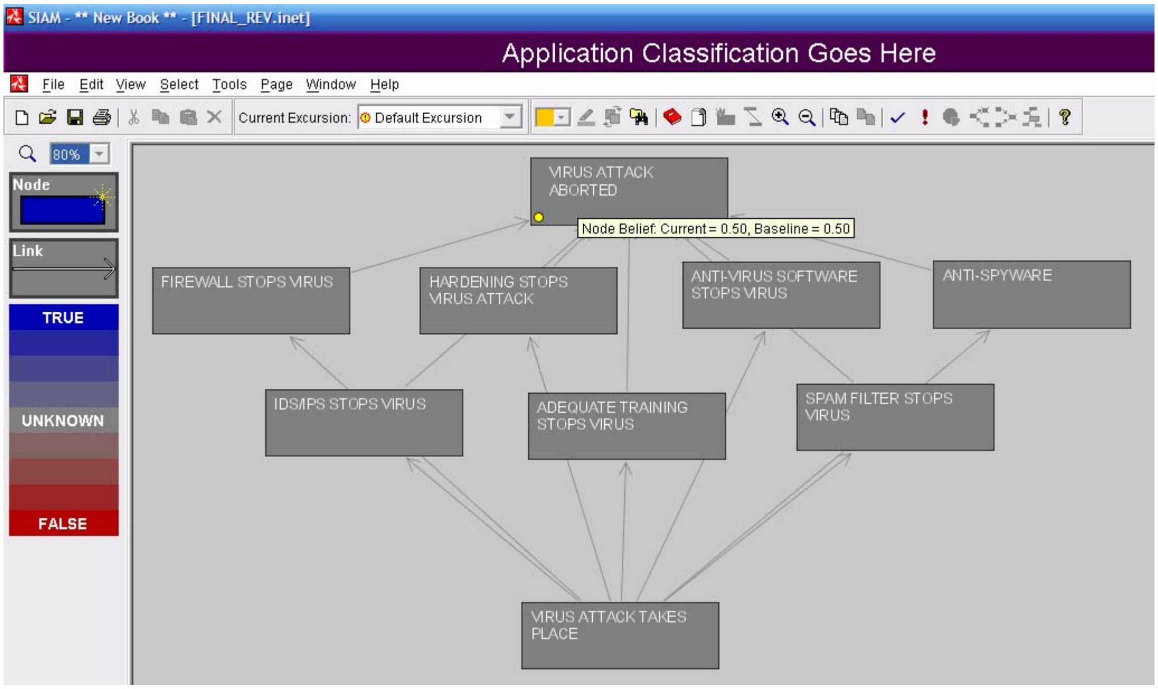
c. Anti-virus software

d. Anti-spyware software

e. Spam filter

f. Training

g. IDS/IPS



Node Belief: Current = 0.50, Baseline = 0.50

Figure 5. Security Tools and links

In establishing link values for the amount of expected protection a particular security tool provides against common attack methods an expert opinion survey to gather collective experience and compiled opinions was created. The surveys were then distributed to a small group of graduate level instructors at Naval Postgraduate School in fields of computer science and information assurance, as well as to current network IT security personnel working in the field. Each survey was accompanied by a cover letter describing the survey along with some clarification statements, as well as a terms and definitions list to assist in standardizing responses.

The survey was comprised of seven sets of questions. Each set of questions focused on one mitigation tool (i.e., system hardening, use of firewall, IDS/IPS, training, anti-virus software, anti-spam and anti-spyware software) and the probability that tool could prevent a likely attack method. The attacks considered were those listed in the U.S. Army Intelligence Department and described in Chapter II, section E: virus, worm, trojan horse, denial of service, backdoor, keylogger, sniffer, IP address spoofing, E-mail spoofing, logic bomb, and lastly, being taken over and turned into a zombie. A blank copy of the survey questions is contained in Appendix A.

The survey questions were in pairs according to specific security measures. The first question was designed to capture the survey takers judgment of the security measures impact on attack prevention if the measure is employed; the second question was designed to reflect the survey taker's judgment of the impact on not using the security measure. Each question had an eleven category range, spanning from "severely inhibits" to "severely promotes," which, purposefully matches up with SIAM's measurement techniques for assigning linkage values between nodes. Each of the eleven possible selections has a corresponding numerical value for use in the influence net model, with +1 being severely promoting and a -1 corresponding to severely inhibiting. A total of four surveys were returned and the discrete analysis of the results is provided in Appendix B.

The results as shown in Appendix B were then used to assign link values between each of the seven security tools and each of the 13 attack method (outcome) nodes.

In summary, if a virus attack were to take place as illustrated in Figure 5, then that node would be assigned a 100% truth value to indicate an attack taking place. The attack information would then be linked to the seven different security tools, which on their output side were assigned the values corresponding to the likelihood of preventing an attack. Then after the simulation was ran, the node titled, “virus attack aborted” would reflect the likelihood of whether the attack was successfully thwarted given deployment of the security mechanisms. The Bayesian algorithm would then continue through the model to the root node titled, “Ship defends against cyber attack methods” to determine its probability as well.

With all the major parts of the model described and illustrated, the model will be populated with a theoretical situation in the next chapter to demonstrate its possible application.

THIS PAGE INTENTIONALLY LEFT BLANK

V. MODEL DEMONSTRATION AND RESULTS

To demonstrate the model a notional situation was constructed for use in populating the model. The situation is as follows:

> Let’s say a software company in Seattle, WA fires one of their most knowledgably programmers, named Jim, for being habitually late and disrespectful to other employees. Aside from being a very skillful programmer, Jim also takes pride in being a pretty savvy hacker and is thrilled to put his skills to work. Earlier that morning Jim, now a disgruntled ex-employee, was stuck behind a slow Navy van which he blames for his not making it to work on-time and subsequently getting fired. Jim, instead of taking his frustrations out in a healthy and legal manner, decides to try and pay back the local Navy by hacking into an Everett based ship’s network to conduct a virus and worm attack to cause havoc and attempt to bring down the ship’s network.

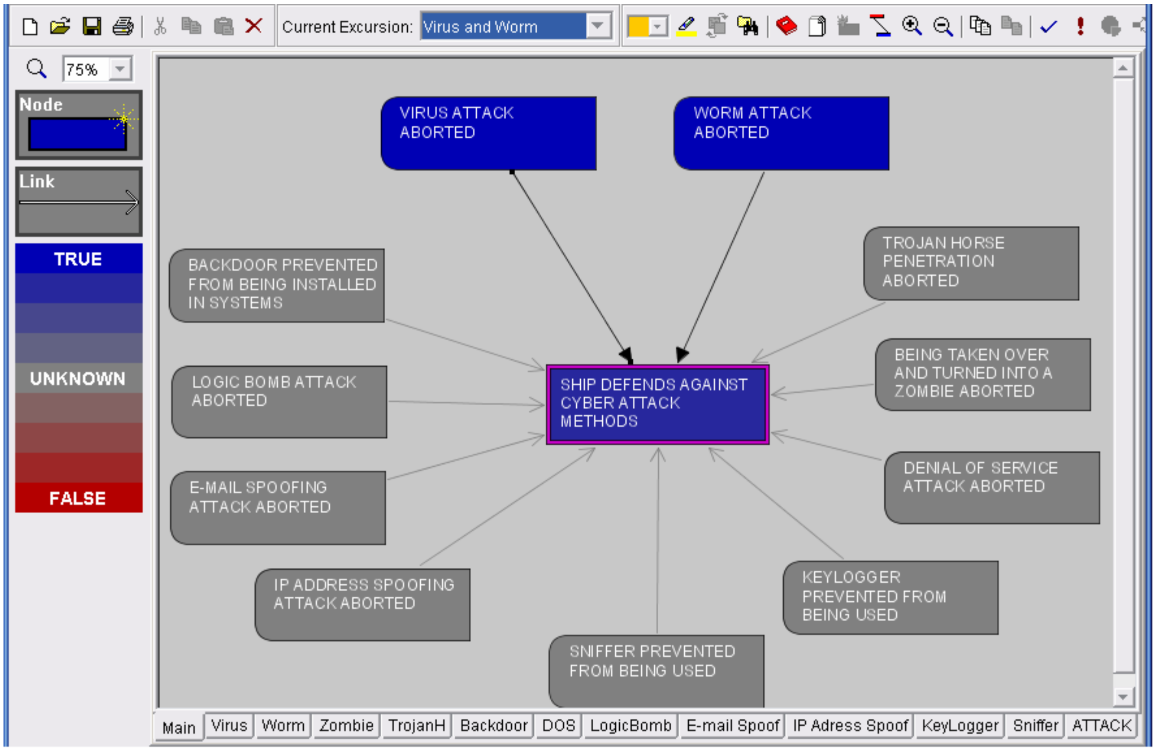
The above scenario describes a hacker with both a strong motive as well as the means to conduct an attack. The opportunity is also available since Jim has access to a computer which is connected to the Internet. The potential success of the attack thus depends almost entirely on the ship’s vulnerabilities and the effectiveness of the mitigation tools used. As was shown in an earlier chapter of this thesis, numerous vulnerabilities exist that if not properly mitigated can be exploited, thus leading to a successful attack.

With the previous chapter providing a detailed description of the initial model construction and the above scenario, the remainder of this chapter will focus on populating the model with the scenario results and running three separate excursions, or examples to show the models versatility as well as to show the likelihood of successful attacks based on different criteria. The first excursion was designed to show how effective the attack would be with all primary mitigation tools in place. The second excursion was designed to show how effective the attack would be if the ship did not utilize anti-virus software. The last excursion was set-up to show the likelihood of a successful attack if no firewall is utilized.

A. EXCURSION ONE

1. All Security Measures Utilized

For this demonstration the aforementioned scenario of a virus and worm attack takes place. Therefore, the initial nodes, "Virus Attack Takes Place" and "Worm Attack Takes Place" were both set to true in order to indicate that the attack took place. Next, the linkages between the attack nodes utilized, and each of the mitigation tools were set to "Severely Promotes the Conclusion," to allow 100% of the attack to take place. The next step was to assign the linkages between each particular mitigation tool and its likelihood of stopping the attack method which were inferred from the expert opinion survey results (Appendix A). The model was then run and provided the following figure and results:



Current Excursion: Virus and Worm

75%
Node
Link
TRUE
UNKNOWN
FALSE
VIRUS ATTACK ABORTED
WORM ATTACK ABORTED
TROJAN HORSE PENETRATION ABORTED
BACKDOOR PREVENTED FROM BEING INSTALLED IN SYSTEMS
BEING TAKEN OVER AND TURNED INTO A ZOMBIE ABORTED
LOGIC BOMB ATTACK ABORTED
SHIP DEFENDS AGAINST CYBER ATTACK METHODS
DENIAL OF SERVICE ATTACK ABORTED
E-MAIL SPOOFING ATTACK ABORTED
IP ADDRESS SPOOFING ATTACK ABORTED
KEYLOGGER PREVENTED FROM BEING USED
SNIFFER PREVENTED FROM BEING USED
Main
Virus
Worm
Zombie
TrojanH
Backdoor
DOS
LogicBomb
E-mail Spoof
IP Adress Spoof
KeyLogger
Sniffer
ATTACK

Figure 6. Excursion 1 (All security measures used)

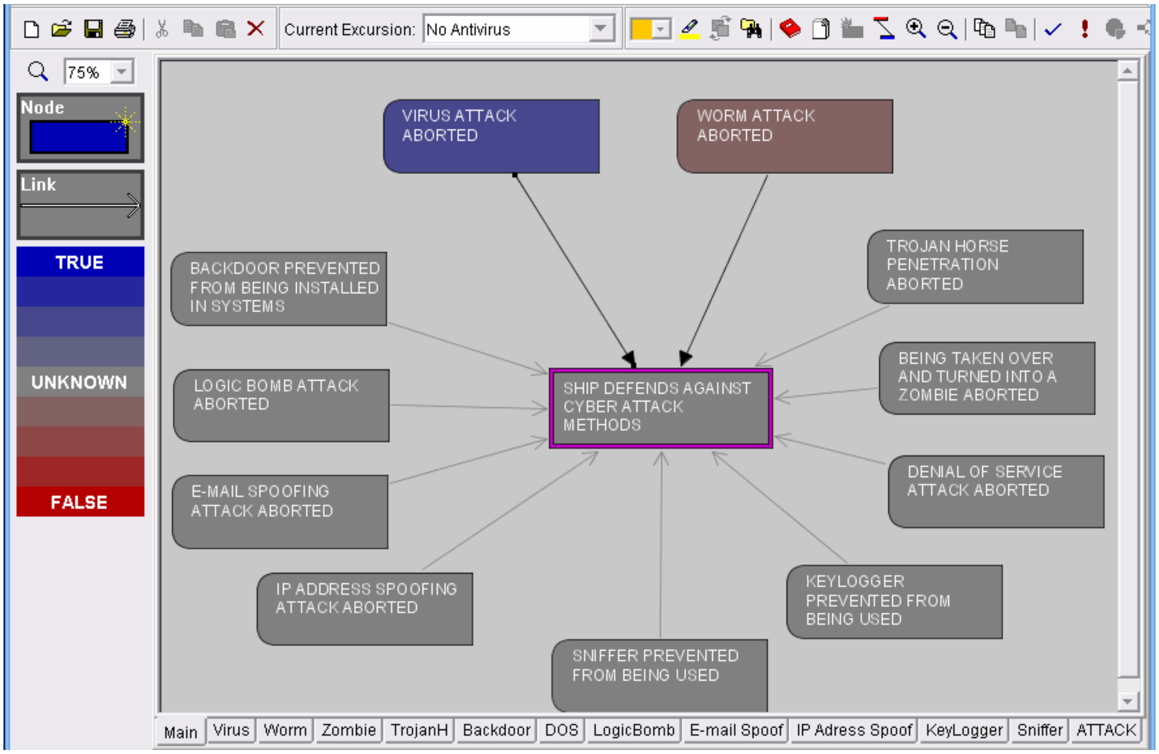
2. **Results**: "Virus Attack Aborted" and "Worm Attack Aborted" were both determined to have a belief value of .99, and the root node, "Ship Defends Against Cyber Attack Methods" was determined to have a belief value of .87. By looking at the color table to the left of Figure 6, we can confirm similar results at a glance. The dark blue colors would translate to the belief "I am extremely certain that this is a true statement."

By interpreting these results the reader should be convinced that the tools in place should protect the ship from attack, however, they also show that the prevention of attack is not 100 percent, therefore, even with all protections in place the possibility of attack does exist. As we will see next, the following results will not be as comforting.

B. EXCURSION TWO

1. No Anti-Virus

For this demonstration the same virus and worm attack occurred, however, this time the protection of the anti-virus software was removed from the equation. To do so the link between the causal node, "Virus Attack Takes Place" and the effect node "Anti-Virus Software Stops Virus" is assigned a value of -1. This then propagates through the model setting the "Anti-virus Software Stops Virus" node to -1, which indicates "I am extremely certain this is a false statement," thereby allowing the virus attack to propagate through the model with no impact from that node. The model was then run again and provided the following figure and results:



Current Excursion: No Antivirus

75%
Node
Link
TRUE
UNKNOWN
FALSE
VIRUS ATTACK ABORTED
WORM ATTACK ABORTED
BACKDOOR PREVENTED FROM BEING INSTALLED IN SYSTEMS
TROJAN HORSE PENETRATION ABORTED
LOGIC BOMB ATTACK ABORTED
SHIP DEFENDS AGAINST CYBER ATTACK METHODS
BEING TAKEN OVER AND TURNED INTO A ZOMBIE ABORTED
E-MAIL SPOOFING ATTACK ABORTED
DENIAL OF SERVICE ATTACK ABORTED
IP ADDRESS SPOOFING ATTACK ABORTED
KEYLOGGER PREVENTED FROM BEING USED
SNIFFER PREVENTED FROM BEING USED
Main
Virus
Worm
Zombie
TrojanH
Backdoor
DOS
LogicBomb
E-mail Spoof
IP Adress Spoof
KeyLogger
Sniffer
ATTACK

Figure 7. Excursion 2 (No anti-virus software used)

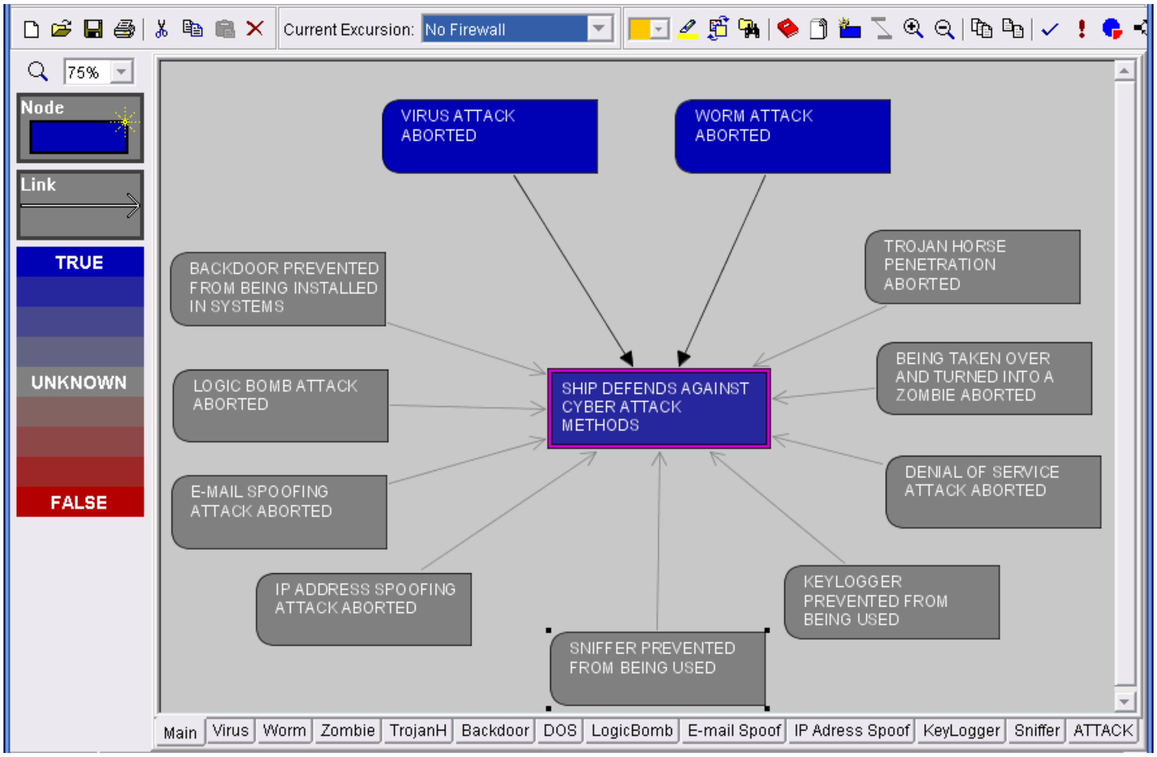
2. Results

"Virus Attack Aborted" was determined to have a belief value of .69, or a synopsis of "I am reasonably certain that this is a true statement." The node "Worm Attack Aborted" was determined to have a belief value of .38, or a synopsis of "I am slightly certain that this is a false statement." The overall root node had a belief value of .53, or unknown value. Again by looking at the color table on the left side of Figure 7, we should be able to make a similar determination. The worm attack node is a light shade of red instead of dark blue, and the virus attack node is about two to three shades lighter of blue. These results indicate that with no Anti-virus protection there is a 31% likelihood that the virus would have gotten through and a 62% likelihood that the worm attack would be successful. In conclusion, the results of the model show that the anti-virus software is more effective at stopping a worm attack than a virus attack, as well as showing that with no anti-virus protection the probability of aborting a virus or worm attack is substantially reduced. The overall likelihood that the ship could defend against this dual attack with no anti-virus was approximately 50%, thus, leading to the final conclusion - that employing updated anti-virus software is a vital mitigation tool against worms and a very good tool for protecting against virus attack. Though Anti-virus protection does prove to provide a large percentage of protection for the above scenario, the aggregate of the other mitigation tools can not be discounted since they do add up to greater than 65% protection in defense of a virus and 35% for a worm. The next excursion was then set-up to show the effect of having no firewall.

C. EXCURSION THREE

1. No Firewall

For this demonstration the same virus and worm attack occurred once again, however, this time instead of not utilizing anti-virus software, the effect of the firewall was disabled by following similar steps as Excursion Two. The model resulted in the following figure.



Current Excursion: No Firewall

75%
Node
Link
TRUE
UNKNOWN
FALSE
VIRUS ATTACK ABORTED
WORM ATTACK ABORTED
BACKDOOR PREVENTED FROM BEING INSTALLED IN SYSTEMS
TROJAN HORSE PENETRATION ABORTED
LOGIC BOMB ATTACK ABORTED
SHIP DEFENDS AGAINST CYBER ATTACK METHODS
BEING TAKEN OVER AND TURNED INTO A ZOMBIE ABORTED
E-MAIL SPOOFING ATTACK ABORTED
DENIAL OF SERVICE ATTACK ABORTED
IP ADDRESS SPOOFING ATTACK ABORTED
KEYLOGGER PREVENTED FROM BEING USED
SNIFFER PREVENTED FROM BEING USED
Main
Virus
Worm
Zombie
TrojanH
Backdoor
DOS
LogicBomb
E-mail Spoof
IP Adress Spoof
KeyLogger
Sniffer
ATTACK

Figure 8. Excursion 3 (No firewall used)

2. Results

The belief values for "Virus Attack Aborted" and "Worm Attack Aborted" were both determined to be .97, similar to the .99 results in Excursion 1. The root node was also very similar with a belief value of .85. The color table to the left of Figure 8 shows that the nodes are dark blue once again, and would translate to the belief "I am extremely certain that this is a true statement." These results show that the firewall had very little effect toward protecting against a virus or worm attack, which is consistent with the Appendix B data. Also, in referring to Appendix B we can see that the firewall is an effective tool in protecting against DOS attacks, IP address spoofing and being taken over and turned into a Zombie. Whereas, protecting against viruses and worms the best tools were Anti-virus software and adequate training to personnel. Therefore, if the firewall goes down, and all other security tools are in place the ship is still fairly well protected from a successful worm or virus attack, though the potential for a DOS attack, IP address spoofing, and being taken over and turned into a Zombie significantly increase.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS AND CONCLUSIONS

A few key recommendations are listed below which could improve this research project, starting with model improvements, and then followed by future research recommendations, and lastly the thesis conclusions.

A. RECOMMENDATIONS

1. Model Improvements

The model presented in this thesis overall met nearly all initial expectations, however, to improve its structure and validity for future use, certain points should be taken into consideration.

a. Survey Improvements

The survey utilized was an appropriate approach for a thesis of this scope, it provided expert opinions on the key security practices and their expected effectiveness, and then by taking an average of these results a baseline for assigning link values was established. However, to get a more accurate representation of overall expert opinions, either a much larger sample size of computer security professionals should be taken, or a workshop type forum should be used to collect the best data for incorporation into the model. A workshop consisting of the same experts would allow a forum to discuss all the particular security tools and the entire process in building the model in greater detail. A workshop would also provide a means of discussion and debate, giving experts the opportunity to convince others of their particular view which may be more correct based on experience or more thorough research – possibly coming to a consensus. However, if using the workshop method you need to be aware of "groupthink" issues which the survey style eliminates.

The expert opinion surveys were completed mainly by academic experts in the fields of computer science and information assurance. It would be prudent to conduct further research based on more opinions of those currently working as network security managers and technicians. Those personnel would see on a daily basis the summary logs and data of in-use security mechanisms (i.e., firewalls and IDS/IPS) and see first hand how many worms and viruses etc… were stopped on a given day.

b. Add in All Security Tools and Attack Methods

To keep this model within scope only the most popular mitigation tools and likely cyber attack methods were built into the model. However, future research should attempt to explore all security tools and threats which can then be built into future models.

c. Conduct More Testing of the Model

One scenario of a dual attack (worm and virus) with three variants was run to show the model's functionality and capabilities. The model should now go through an extensive series of scenarios to show its true potential and to demonstrate its usefulness to the US Naval fleet and other services. These scenarios should then be built into information assurance training which will be described next.

2. Recommended Applications

With a good working model constructed, the model can be used to demonstrate the effects security tools have in the prevention of attacks. The training should be designed for senior leadership and system administration personnel. With the demonstration of the model decision makers can now visualize the importance of each security measure in the prevention of various attacks. This visualization should lead to the enhanced awareness of cyber threats as well as the best practices for thwarting attacks. Additionally, with the enhanced awareness, the necessary security dollars required to buy lacking mitigation tools should come. Furthermore, the training will enhance network administrators' and technicians' knowledge as to the importance of updating anti-virus software, enforcing password policies and conducting training for anyone connected to the Internet.

3. Future Research

To further this research the following recommendations are offered:

a. Conduct a Classified Continuation of This Thesis

In an effort to keep this thesis unclassified no specific navy ship or its vulnerabilities were listed (i.e., what operating system and applications it uses), nor what specific security tools they have and use to counter threats. However, if a classified thesis was conducted and a model built based on a specific ship and its factual data, along with utilizing actual risk assessment data for a particular region, and then incorporating that data to assign adversary motives, means and capabilities linkages, the user could also determine the likelihood of an attack, as well as the likelihood of a successful attack.

b. Keep the Model Current

Each particular node and link will need to be researched periodically in order to keep the model up-to-date. Therefore, each station planning to utilize this model should evaluate all their security mechanisms and conduct a thorough product review of each mitigation tools (i.e., firewalls, IDS, anti-malware etc.). Additionally, as better and better technologies are developed the amount of protection of certain tools is likely to go up, therefore a new set of surveys or a workshop will need to be conducted to establish new link values for use in the model.

c. Conduct Cost Benefit Analysis

In order for the Navy to adopt such a program for service wide use, the benefits verses costs must be weighed and the actual cost determined. The SIAM program would need to be purchased from the SAIC corporation and then it would need to be approved for use by a DAA.

B. CONCLUSIONS

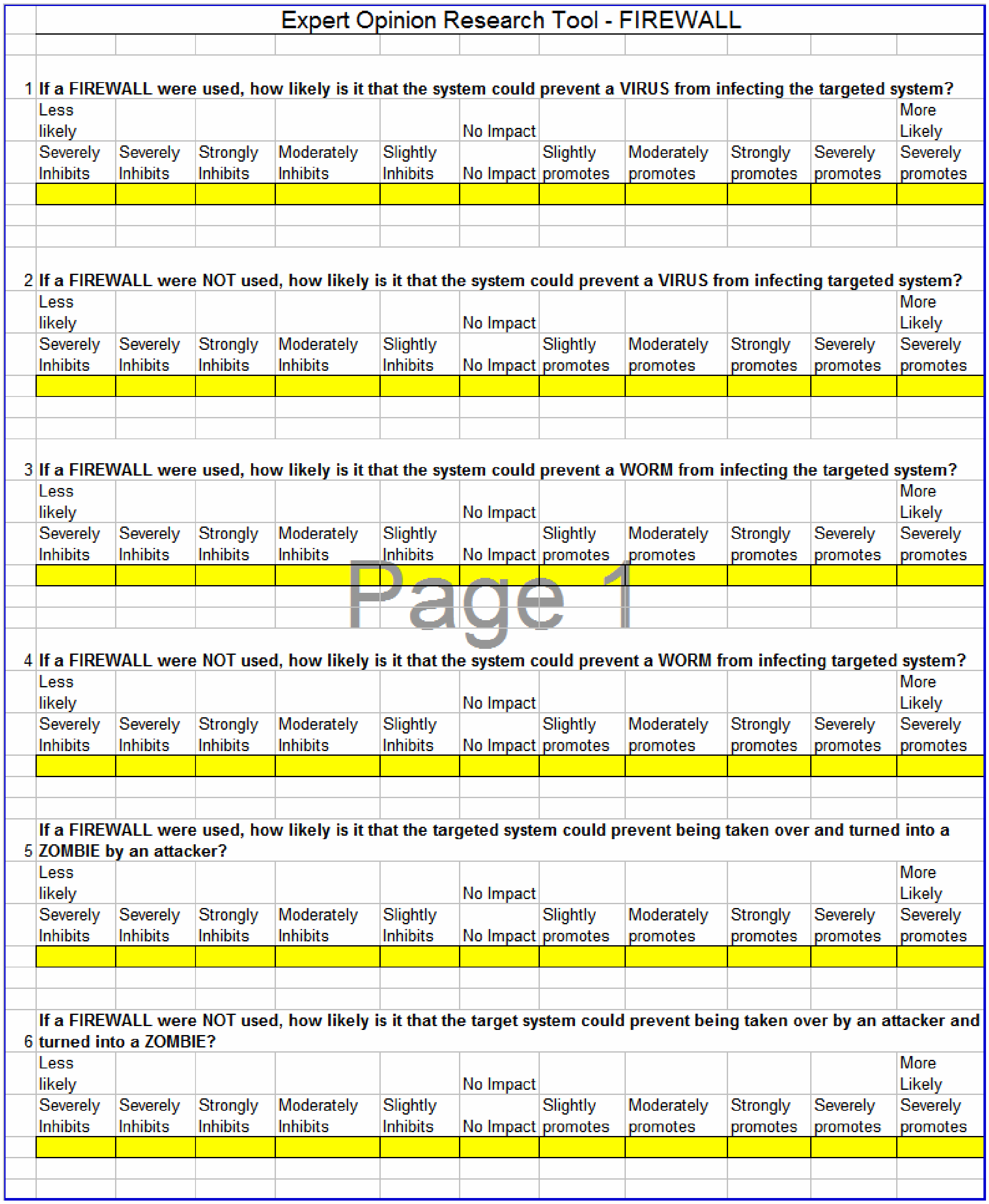
This thesis pointed out the prevalence of cyber attacks, as well as establishing that government computers are not necessarily safe from these attacks. This thesis considered the effects of deploying the best security tools to thwart specific attack methods. The model showed that even with all security tools in place, a ship is still susceptible to attack, however, the risk is much less with the tools in place. This thesis demonstrates a possible means of measuring that risk.

After completing and running the model it proved to be as useful as I had hoped, though a few recommendations as listed in the preceding section could make the model even more useful. Overall, the model does seem to have the key components of a good model such as adequate scope, complexity, and re-use. As far as the scope, I believe this particular model adequately modeled the system to be studied (i.e., network security) and that once populated and run could provide the user with enough information that he/she could make a good decision. Additionally the model was clear and easy to understand, yet complex enough to answer the question of interest. Lastly, the model has re-use potential. In addition to being a good training tool, the model with modification could be used to model any number of threat scenarios and provide the likelihood of their success.

APPENDIX A EXPERT OPINION SURVEY

The following survey was distributed to various Naval Postgraduate School professors in the fields of Computer Science and Information Assurance as well as to technical personnel working as network security administrators. The survey was designed to gather collective experience and compiled opinions of the domain experts; they do not represent product review evaluations of network systems. The data collected was then averaged and used to assign link strength values within the SIAM model. Unfortunately only four surveys were returned. The summary results of all surveys are attached as Appendix B.

1. FIREWALL SECTION OF SURVEY



Expert Opinion Research Tool - FIREWALL

1 **If a FIREWALL were used, how likely is it that the system could prevent a VIRUS from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

2 **If a FIREWALL were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

3 **If a FIREWALL were used, how likely is it that the system could prevent a WORM from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

4 **If a FIREWALL were NOT used, how likely is it that the system could prevent a WORM from infecting targeted system?**

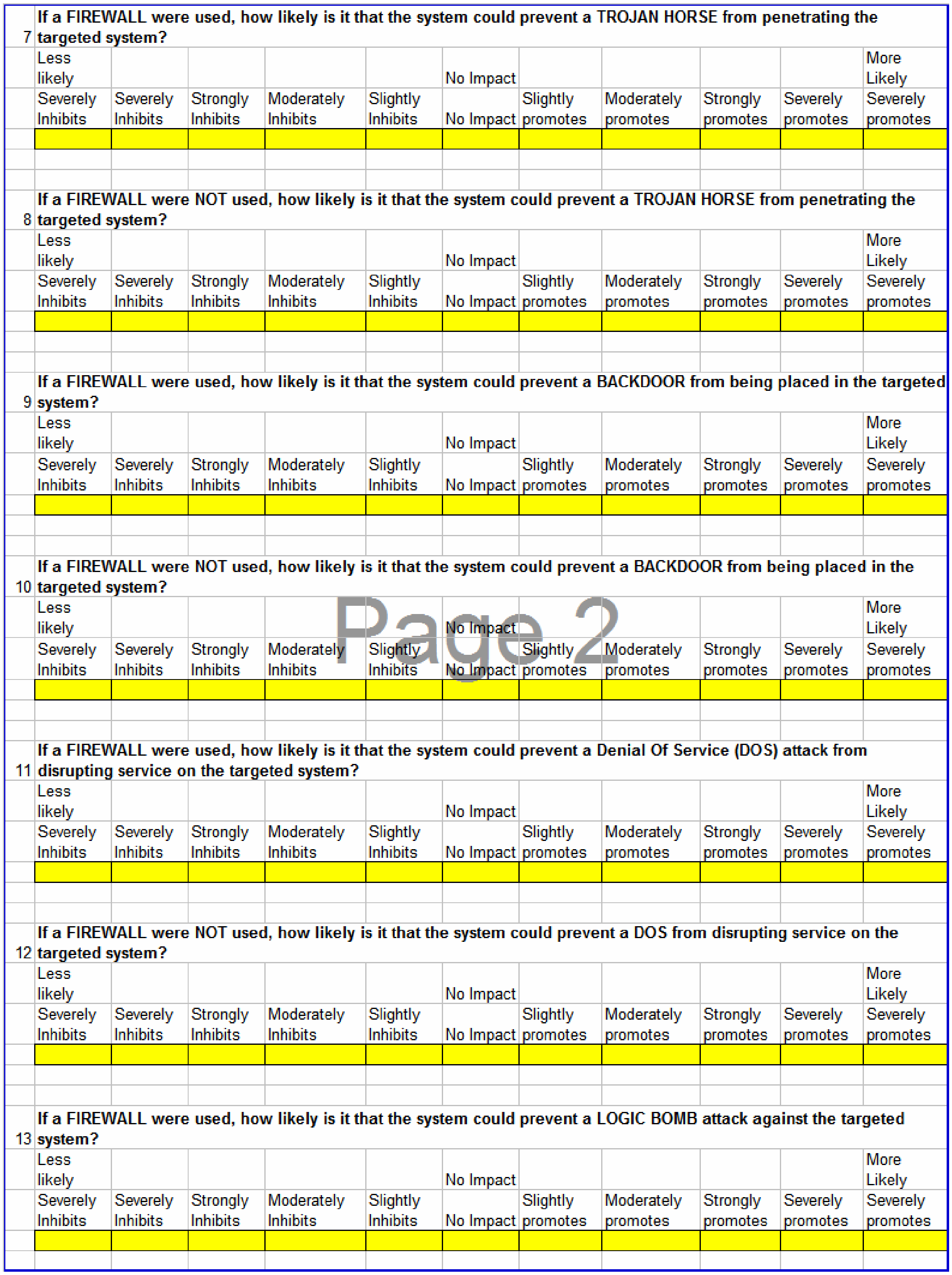
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

5 **If a FIREWALL were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?**

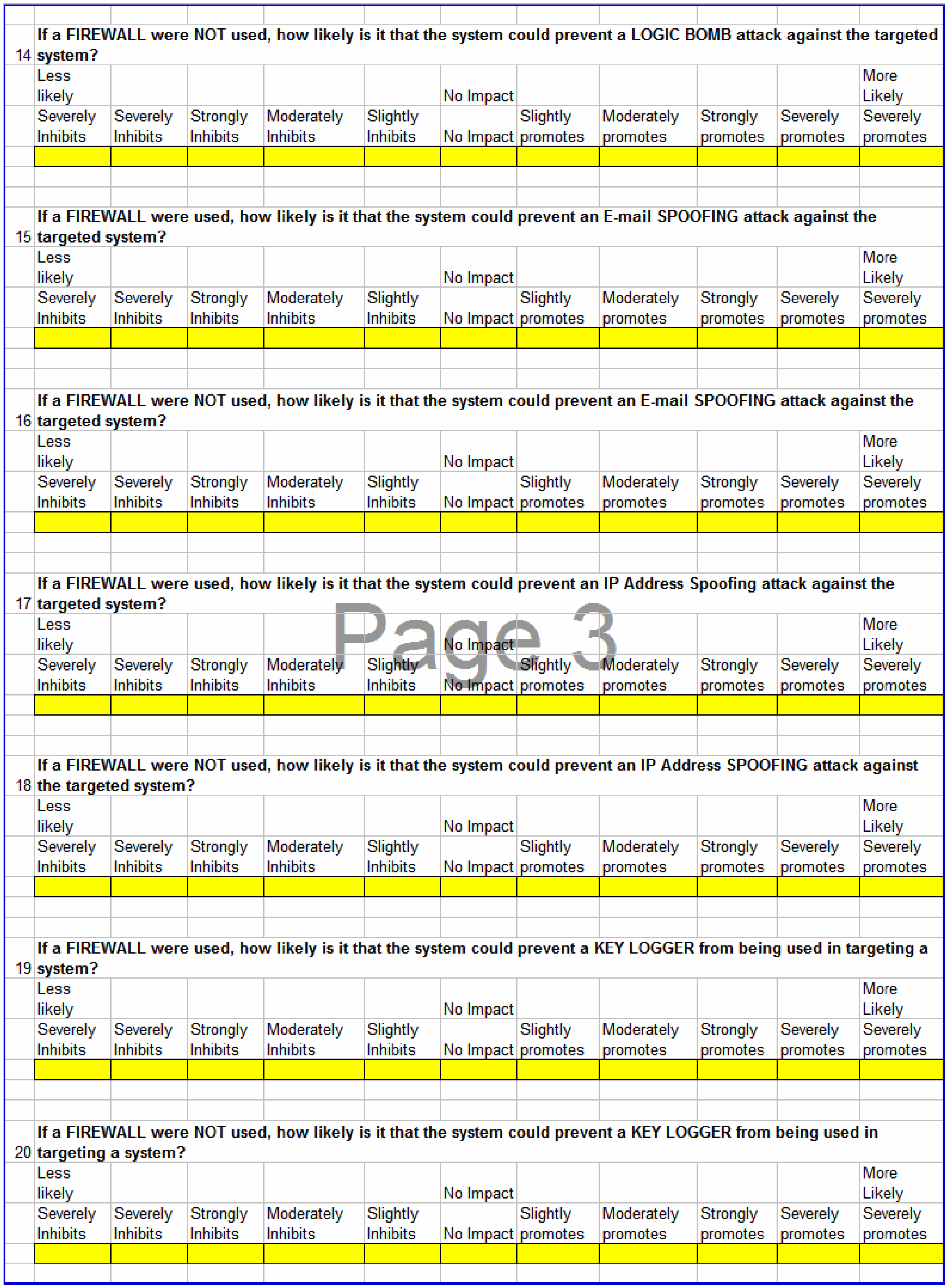
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

6 **If a FIREWALL were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?**

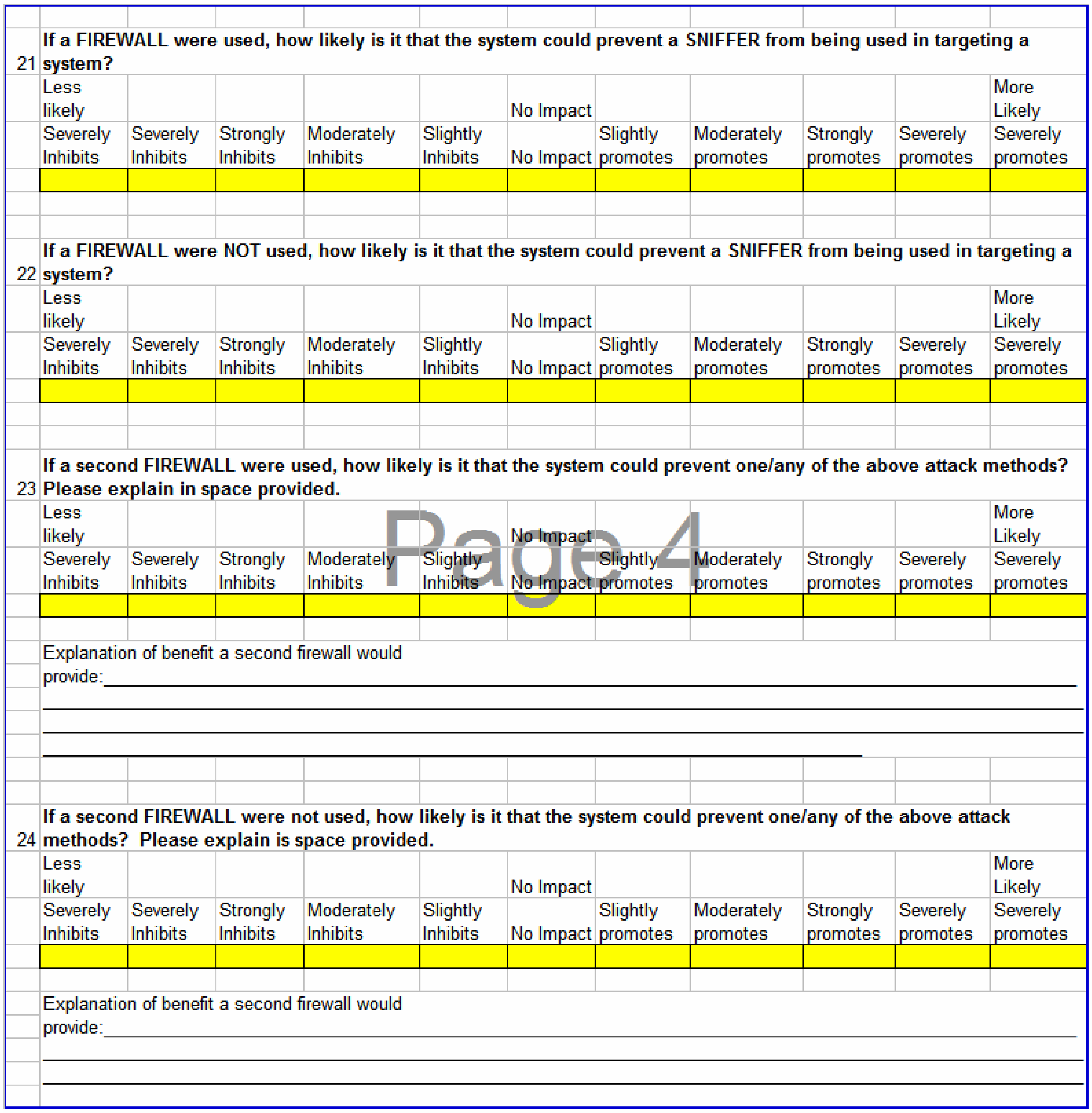
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



7	**If a FIREWALL were used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
8	**If a FIREWALL were NOT used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
9	**If a FIREWALL were used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
10	**If a FIREWALL were NOT used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
11	**If a FIREWALL were used, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
12	**If a FIREWALL were NOT used, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
13	**If a FIREWALL were used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



14	**If a FIREWALL were NOT used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
15	**If a FIREWALL were used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
16	**If a FIREWALL were NOT used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
17	**If a FIREWALL were used, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
18	**If a FIREWALL were NOT used, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
19	**If a FIREWALL were used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
20	**If a FIREWALL were NOT used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



21 **If a FIREWALL were used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

22 **If a FIREWALL were NOT used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

23 **If a second FIREWALL were used, how likely is it that the system could prevent one/any of the above attack methods? Please explain in space provided.**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

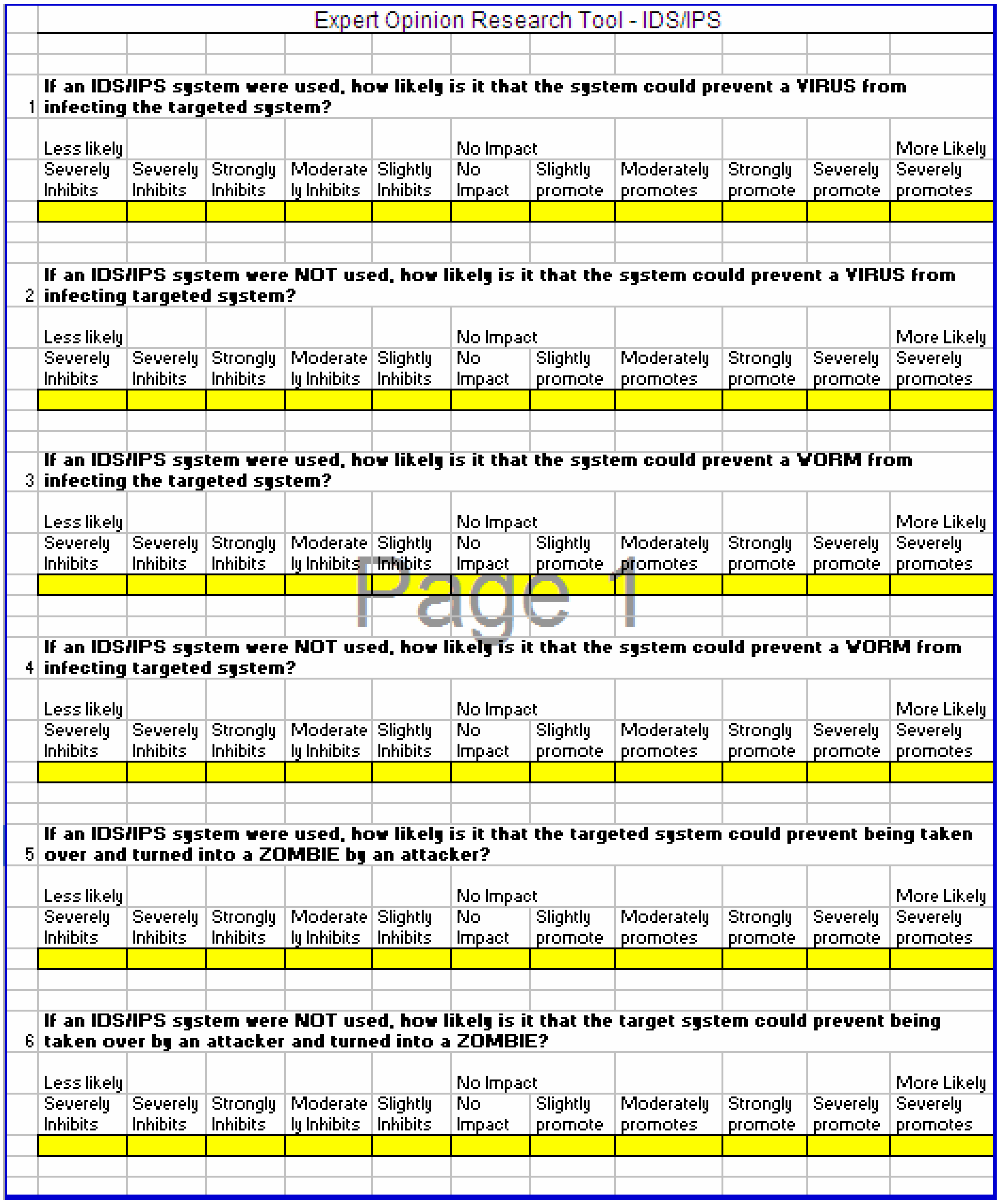
Explanation of benefit a second firewall would provide:____
____
____
____

24 **If a second FIREWALL were not used, how likely is it that the system could prevent one/any of the above attack methods? Please explain is space provided.**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

Explanation of benefit a second firewall would provide:____
____
____

2. IDS/IPS SECTION OF SURVEY



Expert Opinion Research Tool - IDS/IPS

1 If an IDS/IPS system were used, how likely is it that the system could prevent a VIRUS from infecting the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

2 If an IDS/IPS system were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

3 If an IDS/IPS system were used, how likely is it that the system could prevent a WORM from infecting the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

4 If an IDS/IPS system were NOT used, how likely is it that the system could prevent a WORM from infecting targeted system?

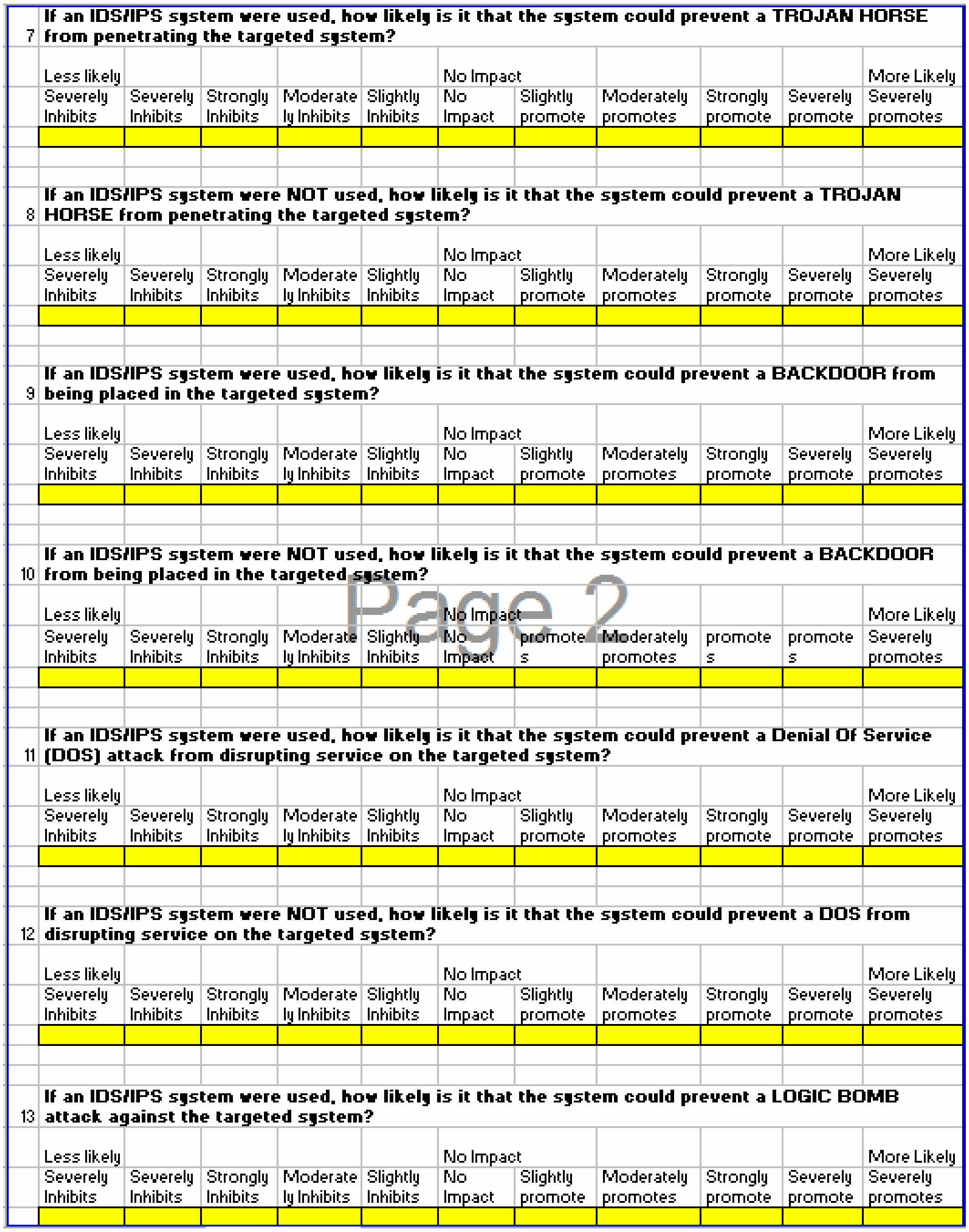
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

5 If an IDS/IPS system were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

6 If an IDS/IPS system were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes



7 **If an IDS/IPS system were used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

8 **If an IDS/IPS system were NOT used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

9 **If an IDS/IPS system were used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

10 **If an IDS/IPS system were NOT used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	promotes	Moderately promotes	promotes	promotes	Severely promotes

11 **If an IDS/IPS system were used, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?**

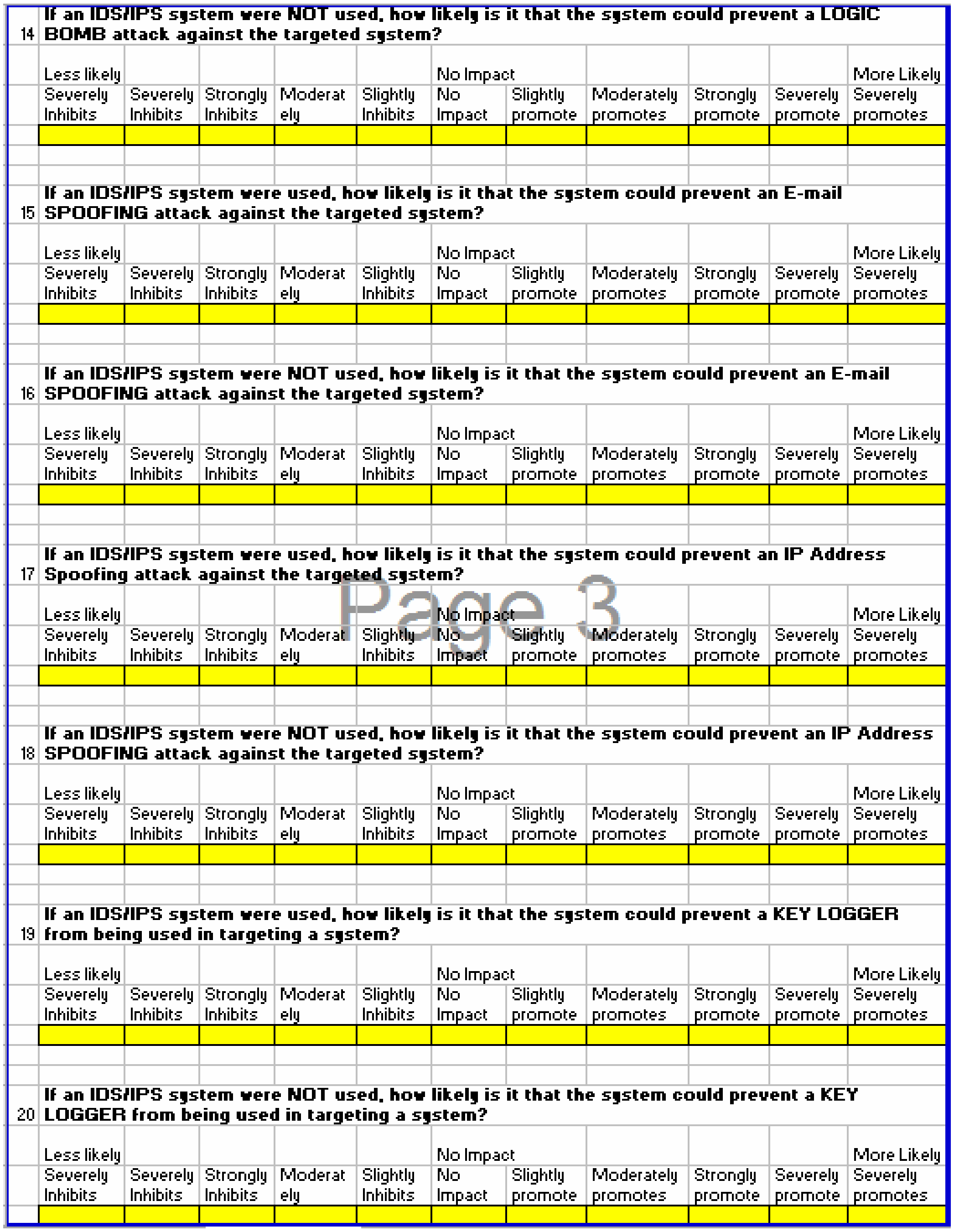
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

12 **If an IDS/IPS system were NOT used, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?**

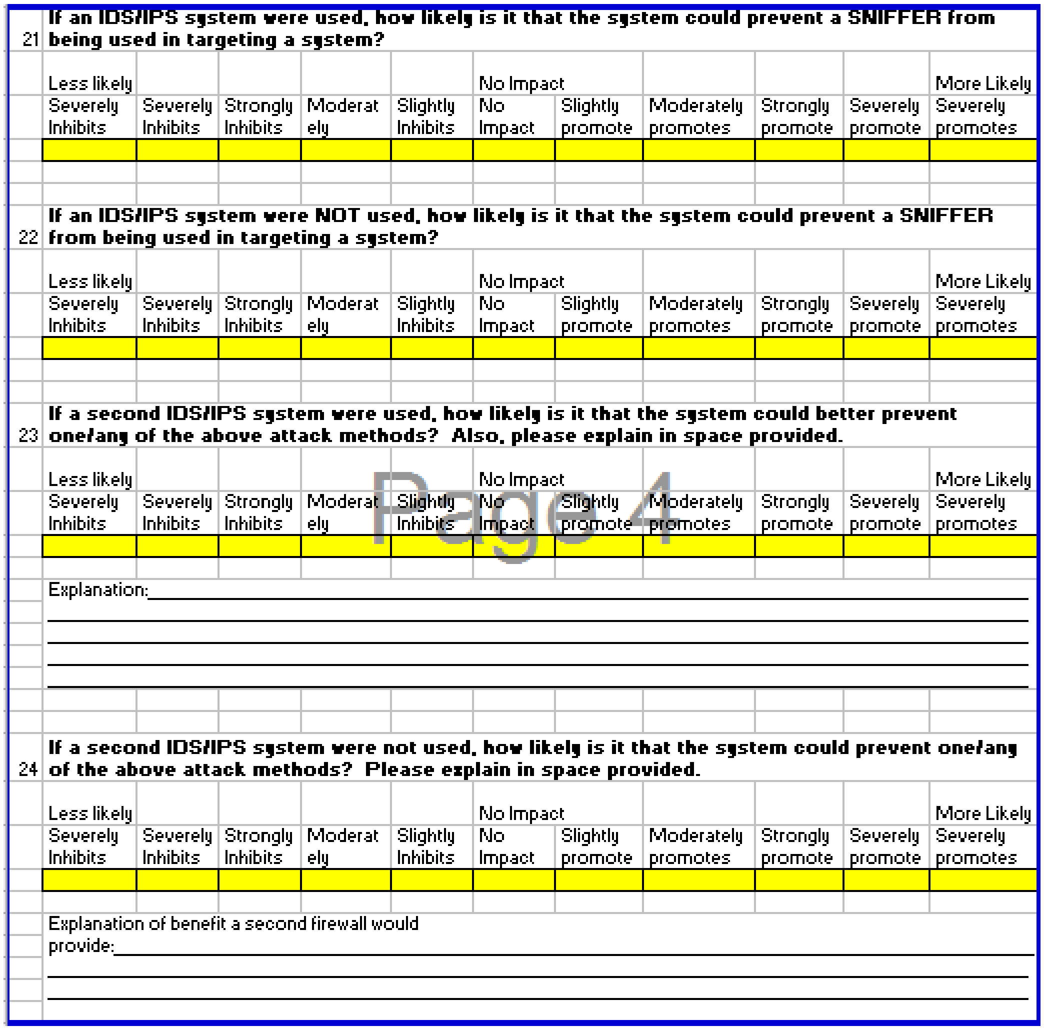
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

13 **If an IDS/IPS system were used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes



14	**If an IDS/IPS system were NOT used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
15	**If an IDS/IPS system were used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
16	**If an IDS/IPS system were NOT used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
17	**If an IDS/IPS system were used, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
18	**If an IDS/IPS system were NOT used, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
19	**If an IDS/IPS system were used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes
20	**If an IDS/IPS system were NOT used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes



21 **If an IDS/IPS system were used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

22 **If an IDS/IPS system were NOT used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

23 **If a second IDS/IPS system were used, how likely is it that the system could better prevent one/any of the above attack methods? Also, please explain in space provided.**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

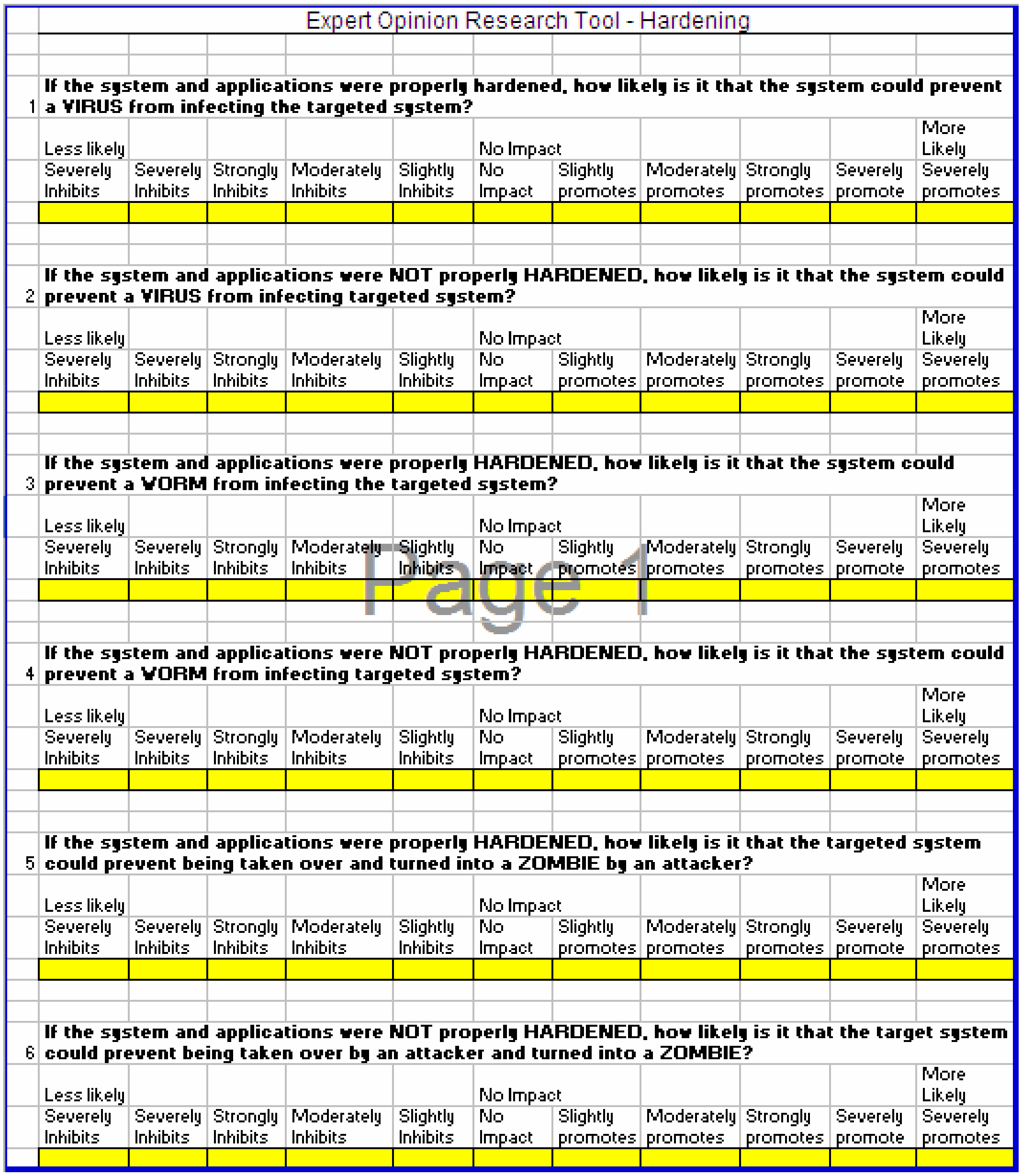
Explanation:

24 **If a second IDS/IPS system were not used, how likely is it that the system could prevent one/any of the above attack methods? Please explain in space provided.**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promote	Severely promotes

Explanation of benefit a second firewall would provide:

3. HARDENING SECTION OF SURVEY



Expert Opinion Research Tool - Hardening

1 If the system and applications were properly hardened, how likely is it that the system could prevent a VIRUS from infecting the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

2 If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a VIRUS from infecting targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

3 If the system and applications were properly HARDENED, how likely is it that the system could prevent a WORM from infecting the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

4 If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a WORM from infecting targeted system?

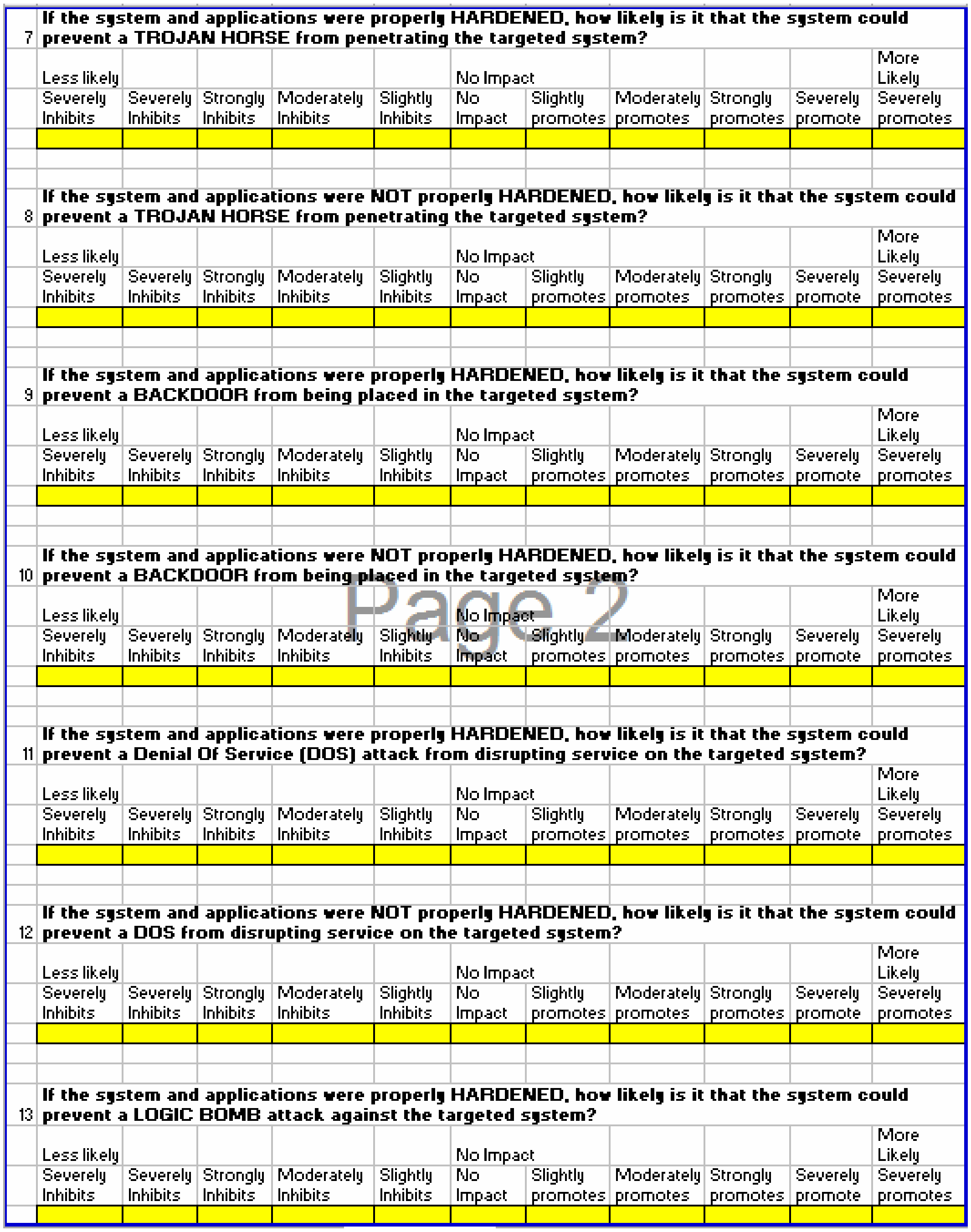
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

5 If the system and applications were properly HARDENED, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?

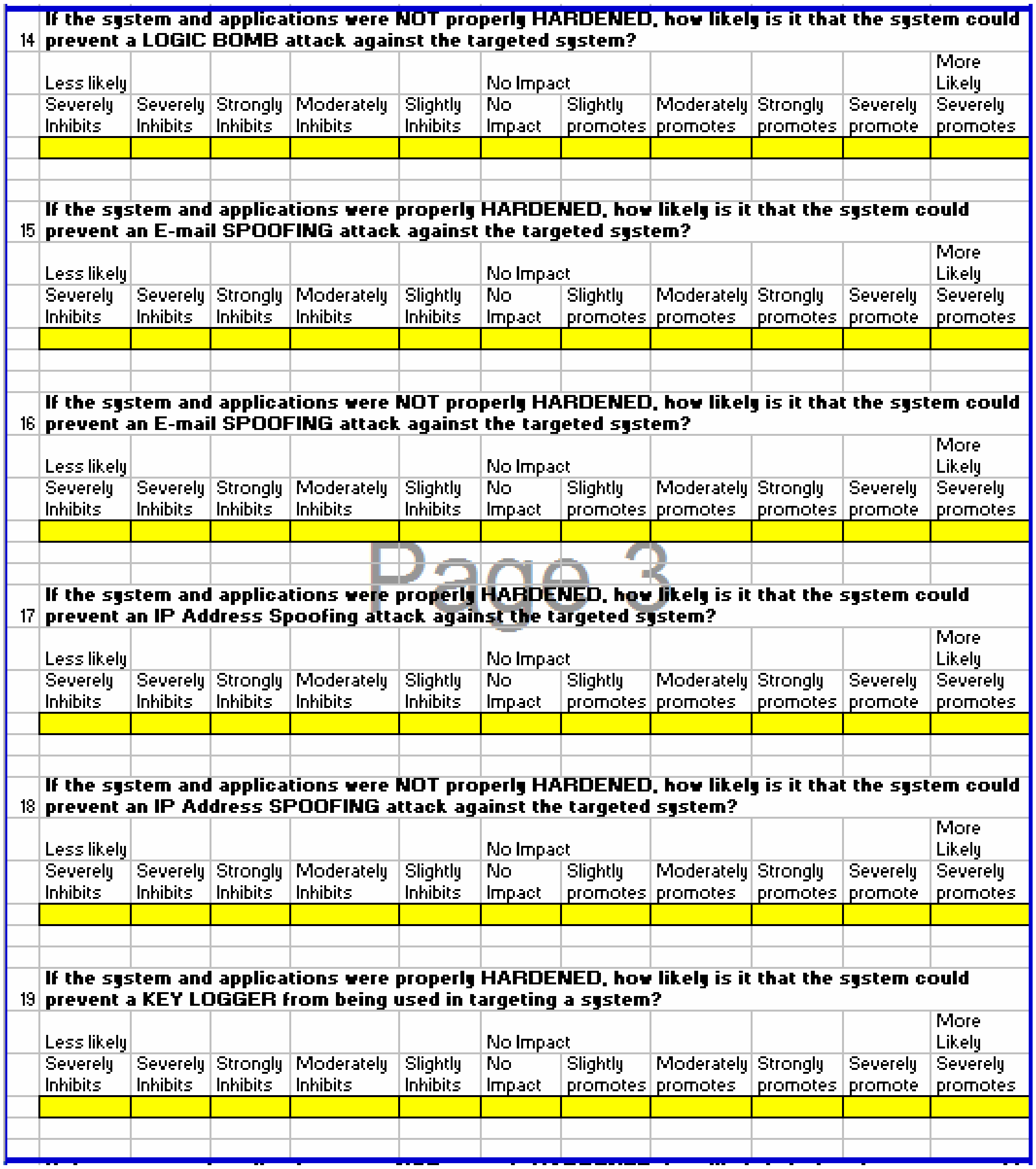
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

6 If the system and applications were NOT properly HARDENED, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?

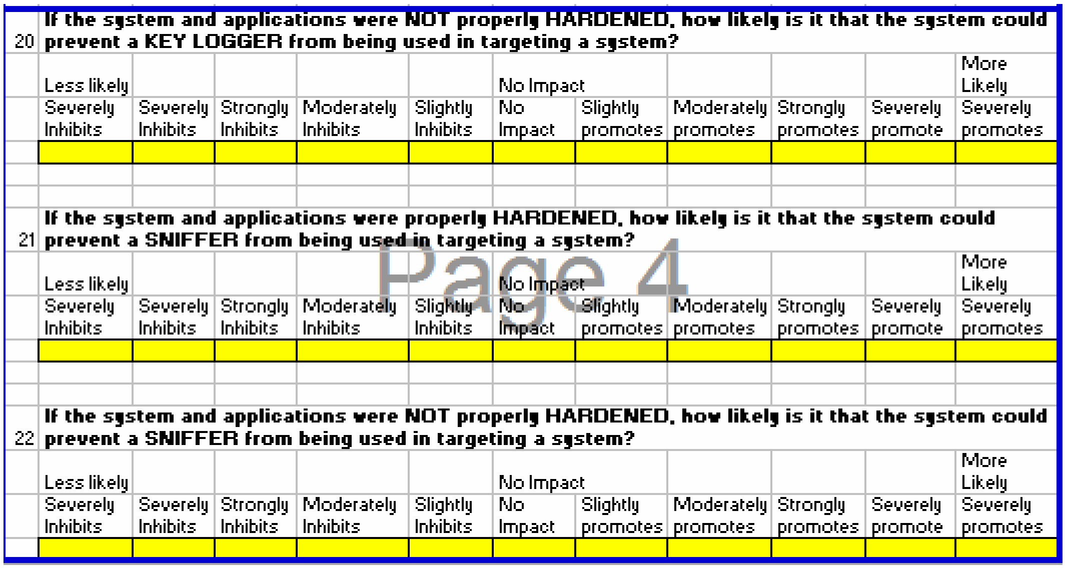
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes



7	If the system and applications were properly HARDENED, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
8	If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
9	If the system and applications were properly HARDENED, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
10	If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
11	If the system and applications were properly HARDENED, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
12	If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
13	If the system and applications were properly HARDENED, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

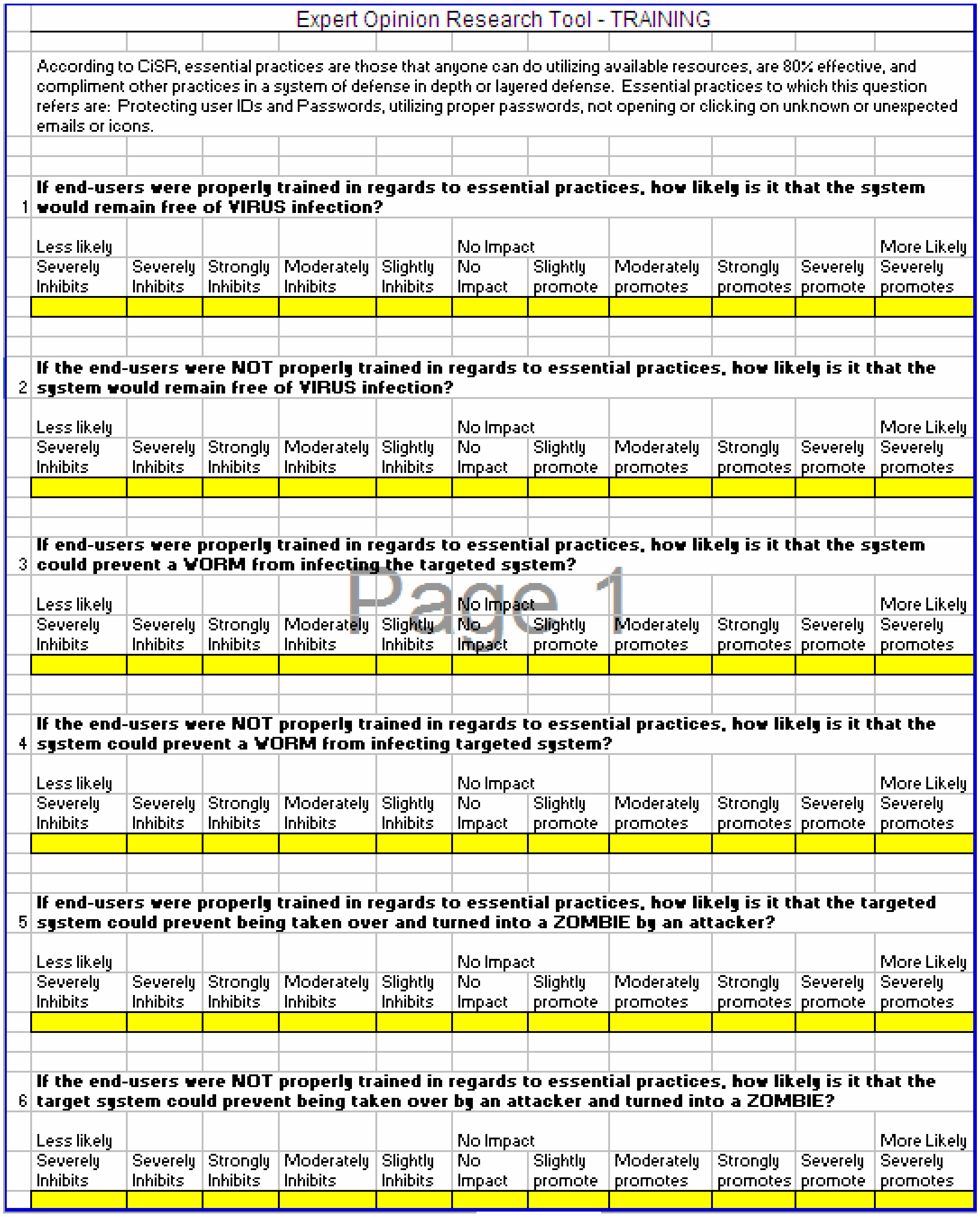


14	**If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
15	**If the system and applications were properly HARDENED, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
16	**If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
17	**If the system and applications were properly HARDENED, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
18	**If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
19	**If the system and applications were properly HARDENED, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes



20	If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
21	If the system and applications were properly HARDENED, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
22	If the system and applications were NOT properly HARDENED, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

4. TRAINING SECTION OF SURVEY



Expert Opinion Research Tool - TRAINING

According to CiSR, essential practices are those that anyone can do utilizing available resources, are 80% effective, and compliment other practices in a system of defense in depth or layered defense. Essential practices to which this question refers are: Protecting user IDs and Passwords, utilizing proper passwords, not opening or clicking on unknown or unexpected emails or icons.

1 **If end-users were properly trained in regards to essential practices, how likely is it that the system would remain free of VIRUS infection?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

2 **If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system would remain free of VIRUS infection?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

3 **If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a WORM from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

4 **If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a WORM from infecting targeted system?**

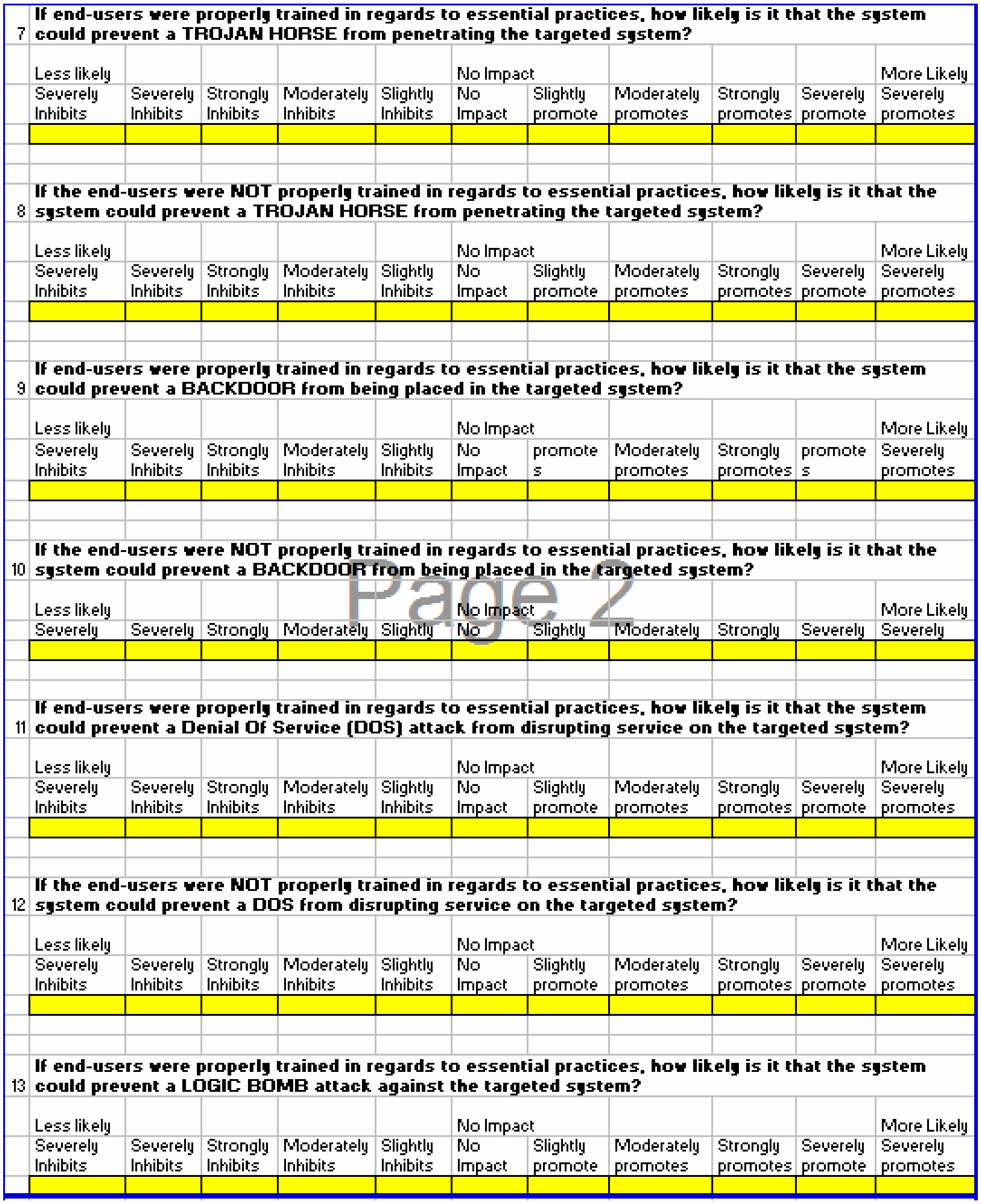
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

5 **If end-users were properly trained in regards to essential practices, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?**

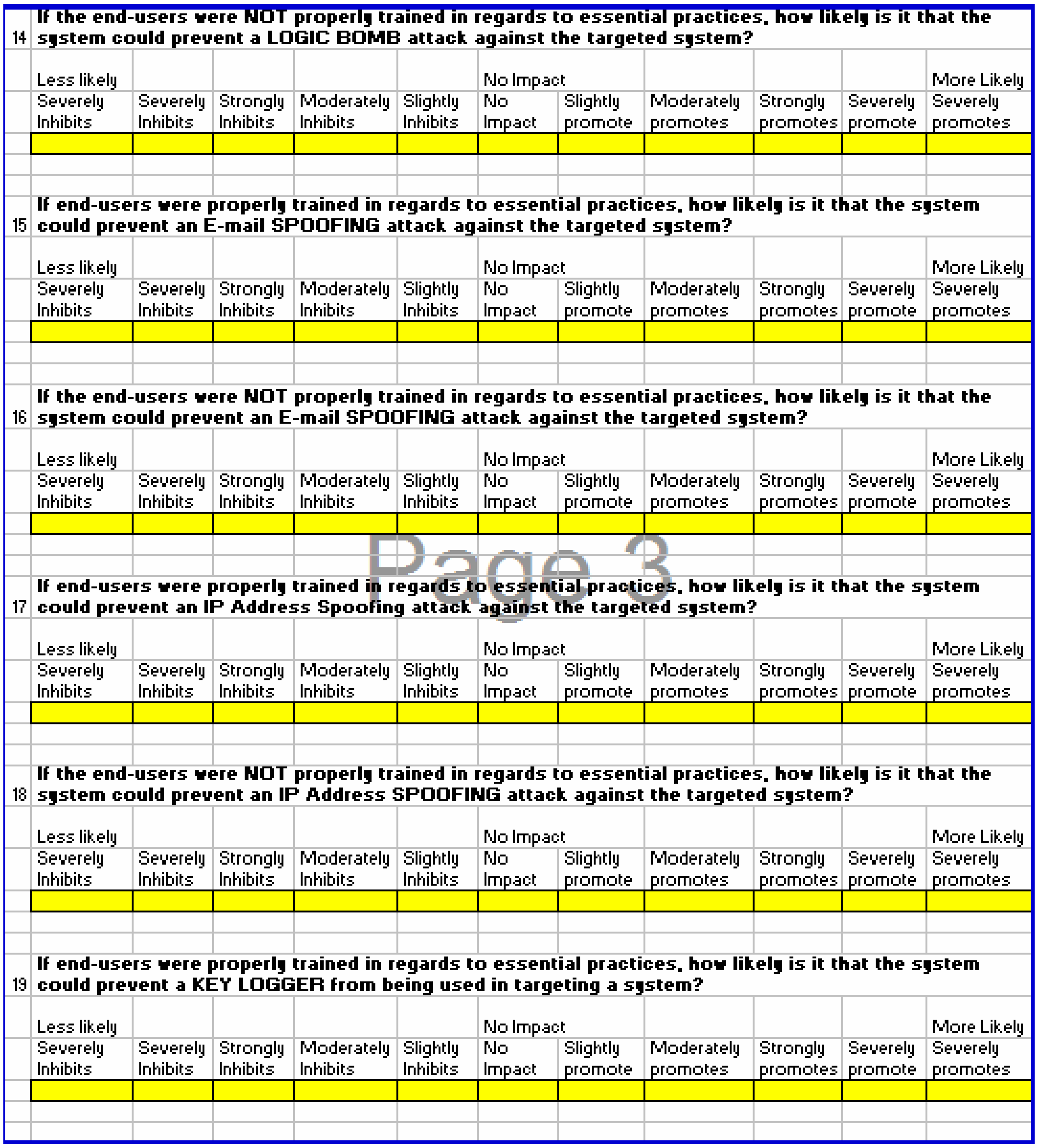
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

6 **If the end-users were NOT properly trained in regards to essential practices, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes



7	If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
8	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
9	If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	promote s	Moderately promotes	Strongly promotes	promote s	Severely promotes
10	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?										
	Less likely					No Impact					More Likely
	Severely	Severely	Strongly	Moderately	Slightly	No	Slightly	Moderately	Strongly	Severely	Severely
11	If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
12	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
13	If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes



14 **If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

15 **If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

16 **If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

17 **If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?**

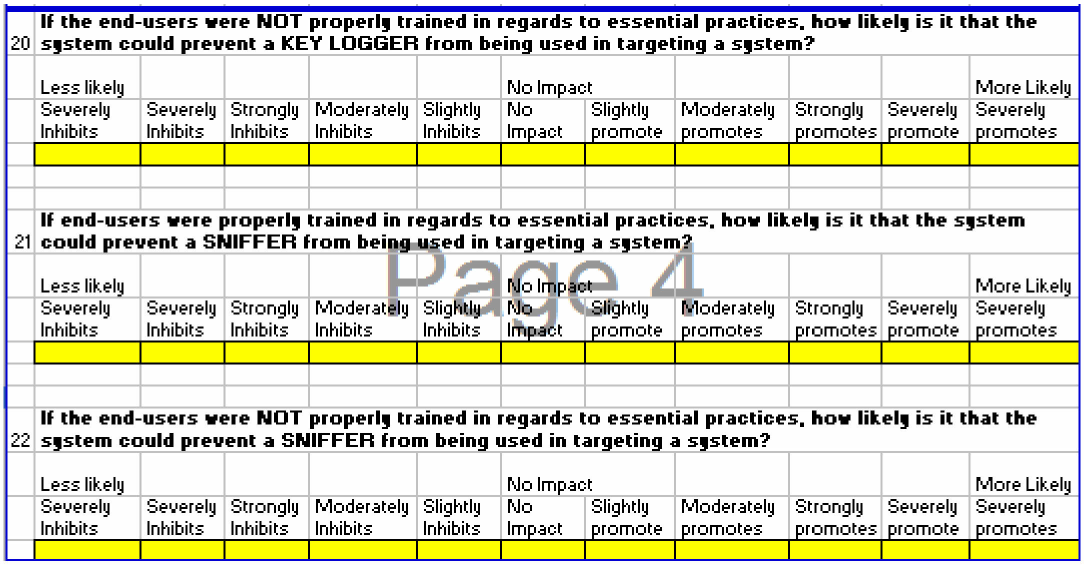
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

18 **If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

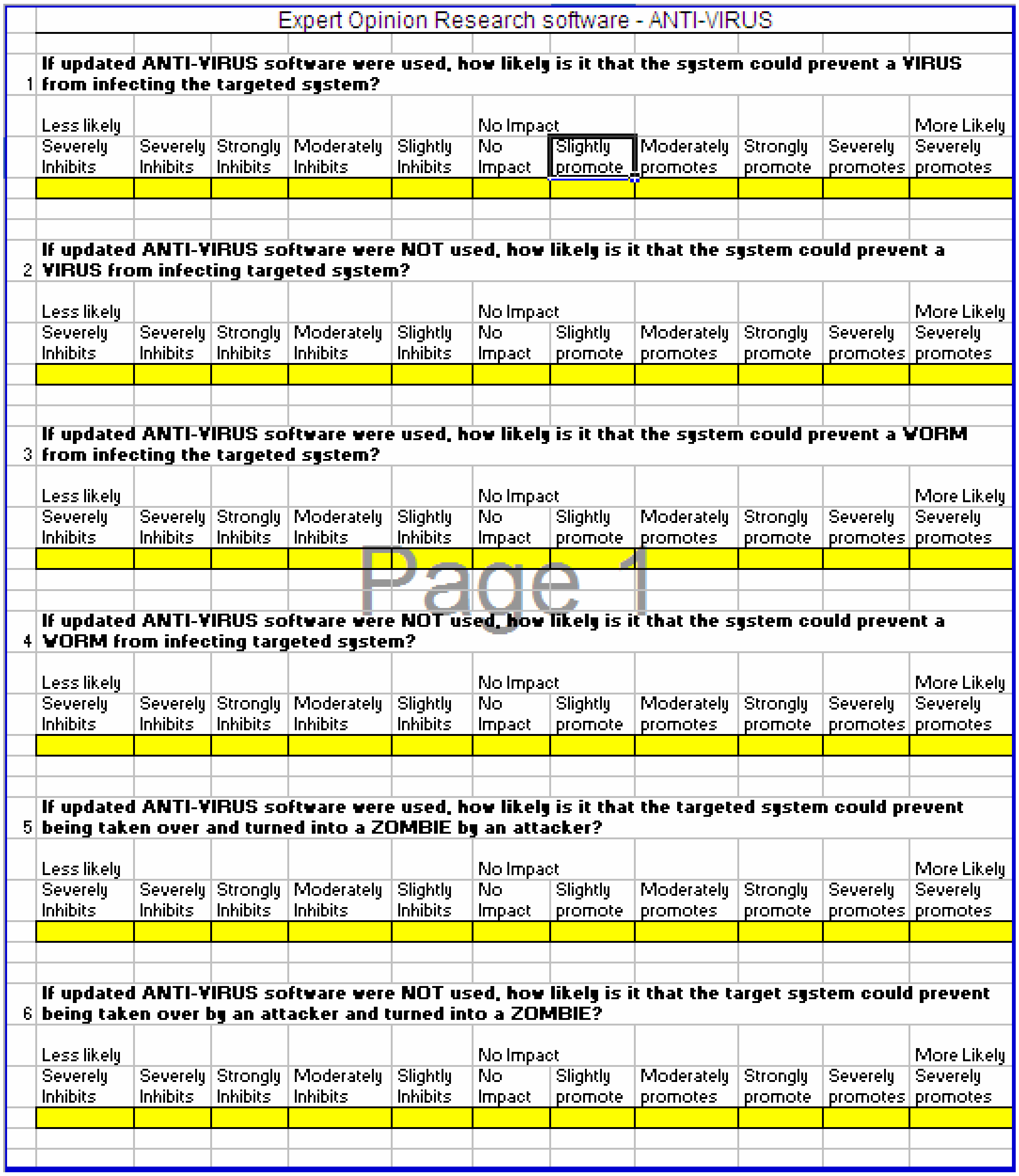
19 **If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes



20	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
21	If end-users were properly trained in regards to essential practices, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes
22	If the end-users were NOT properly trained in regards to essential practices, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promotes	Severely promote	Severely promotes

5. ANTI-VIRUS SECTION OF SURVEY



Expert Opinion Research software - ANTI-VIRUS

1 **If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a VIRUS from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

2 **If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

3 **If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a WORM from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

4 **If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a WORM from infecting targeted system?**

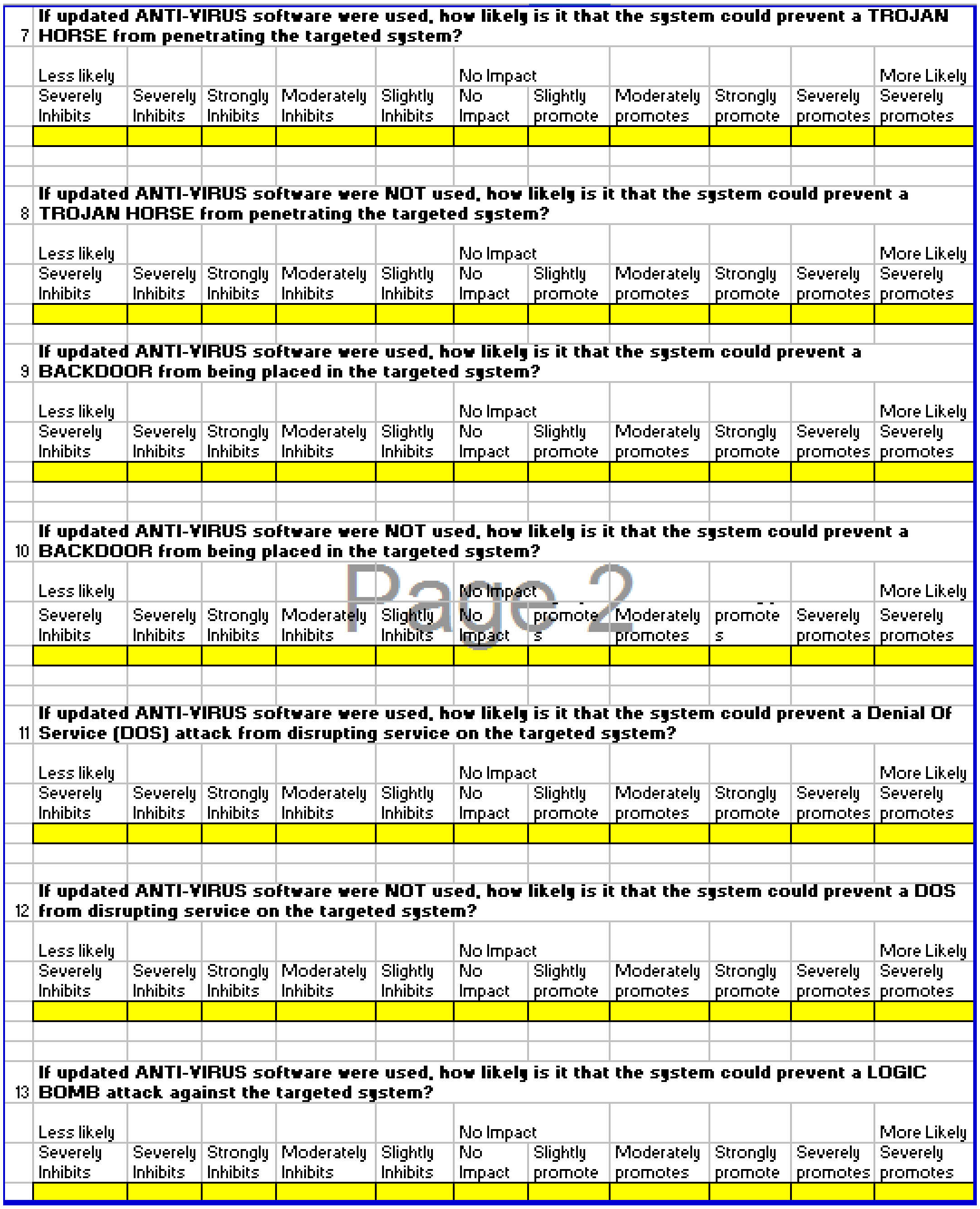
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

5 **If updated ANTI-VIRUS software were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?**

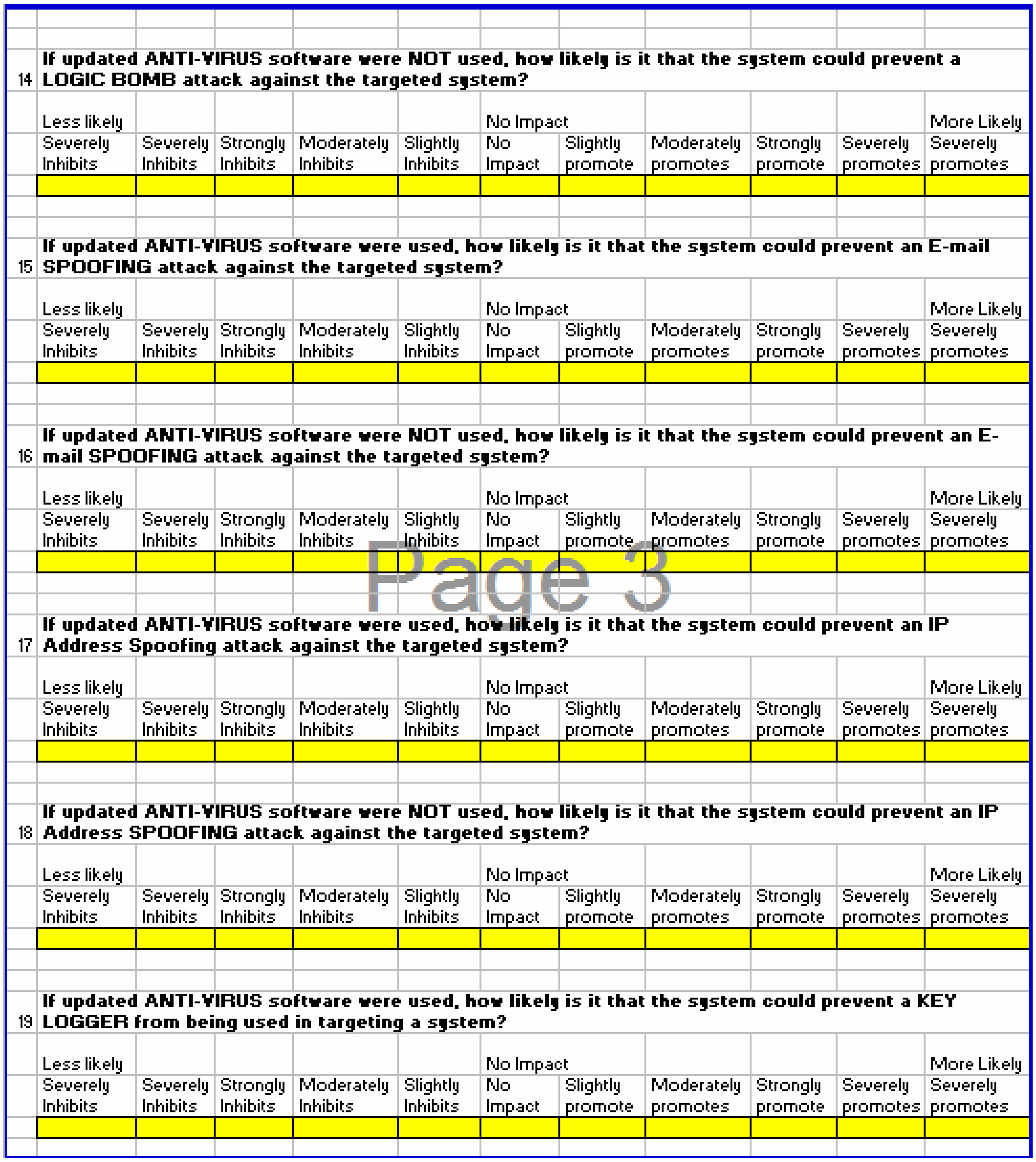
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

6 **If updated ANTI-VIRUS software were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes



7	**If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
8	**If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
9	**If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
10	**If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	promote s	Moderately promotes	promote s	Severely promotes	Severely promotes
11	**If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
12	**If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
13	**If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes



14 **If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

15 **If updated ANTI-VIRUS software were used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

16 **If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

17 **If updated ANTI-VIRUS software were used, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?**

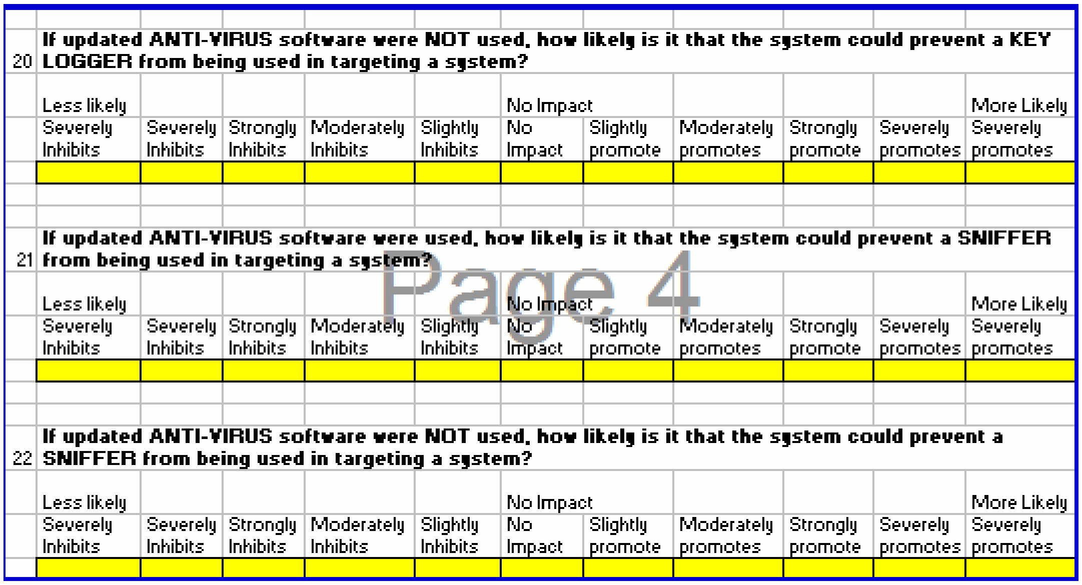
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

18 **If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

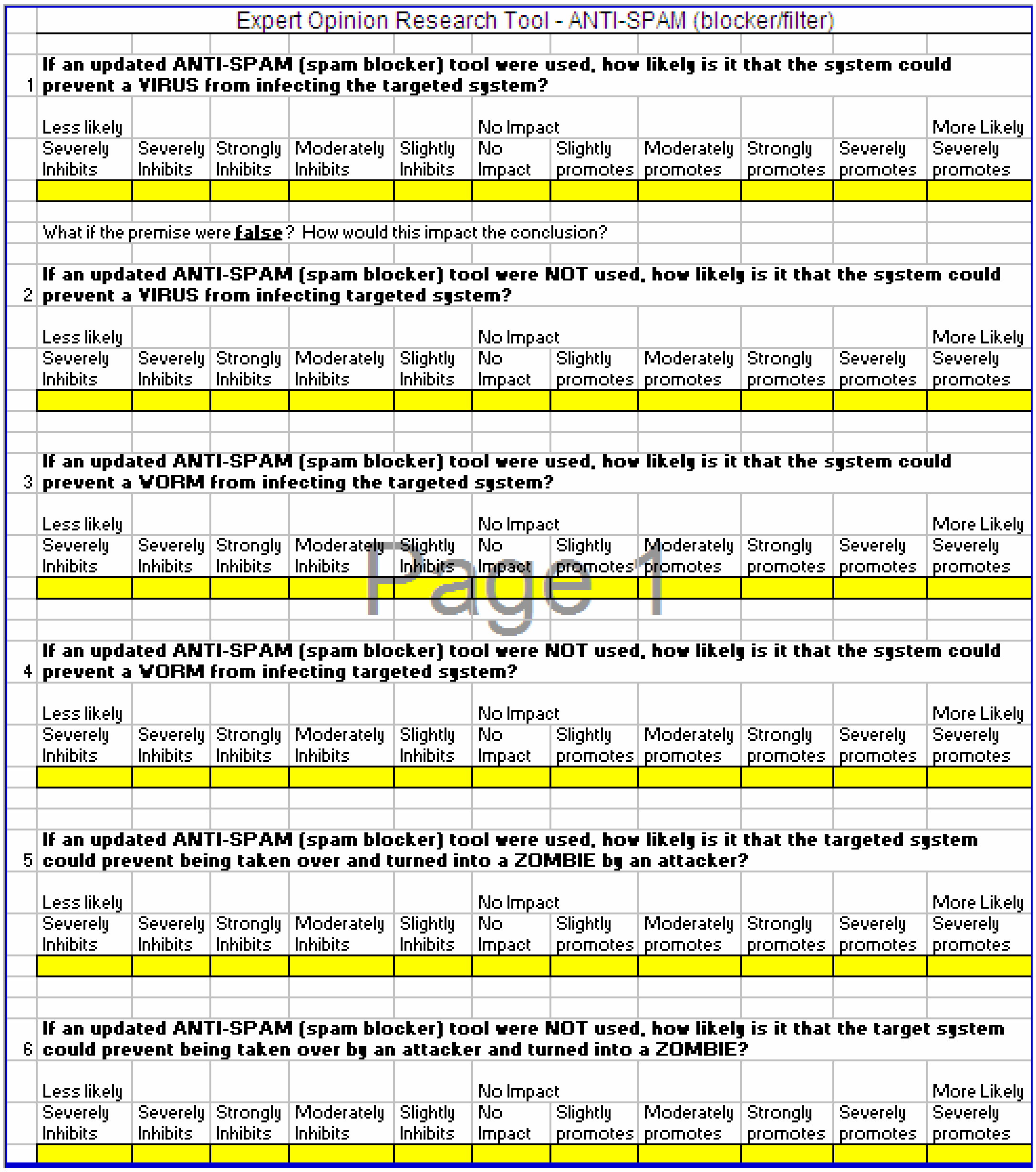
19 **If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes



20	**If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
21	**If updated ANTI-VIRUS software were used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes
22	**If updated ANTI-VIRUS software were NOT used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promote	Moderately promotes	Strongly promote	Severely promotes	Severely promotes

6. ANTI-SPAM SECTION OF SURVEY



Expert Opinion Research Tool - ANTI-SPAM (blocker/filter)

1 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a VIRUS from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

What if the premise were **false**? How would this impact the conclusion?

2 **If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

3 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a WORM from infecting the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

4 **If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a WORM from infecting targeted system?**

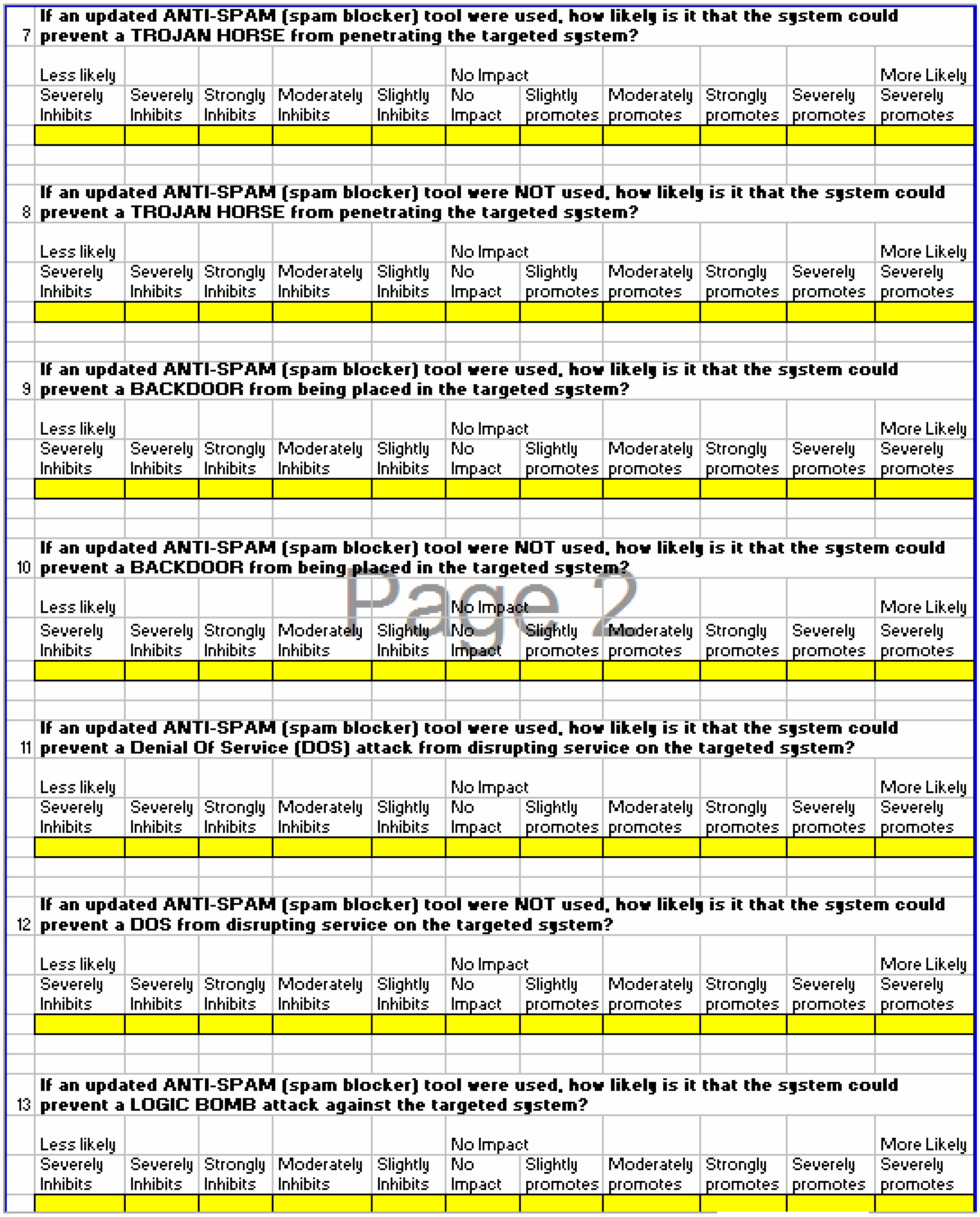
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

5 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

6 **If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



7 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

8 **If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

9 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

10 **If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

11 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?**

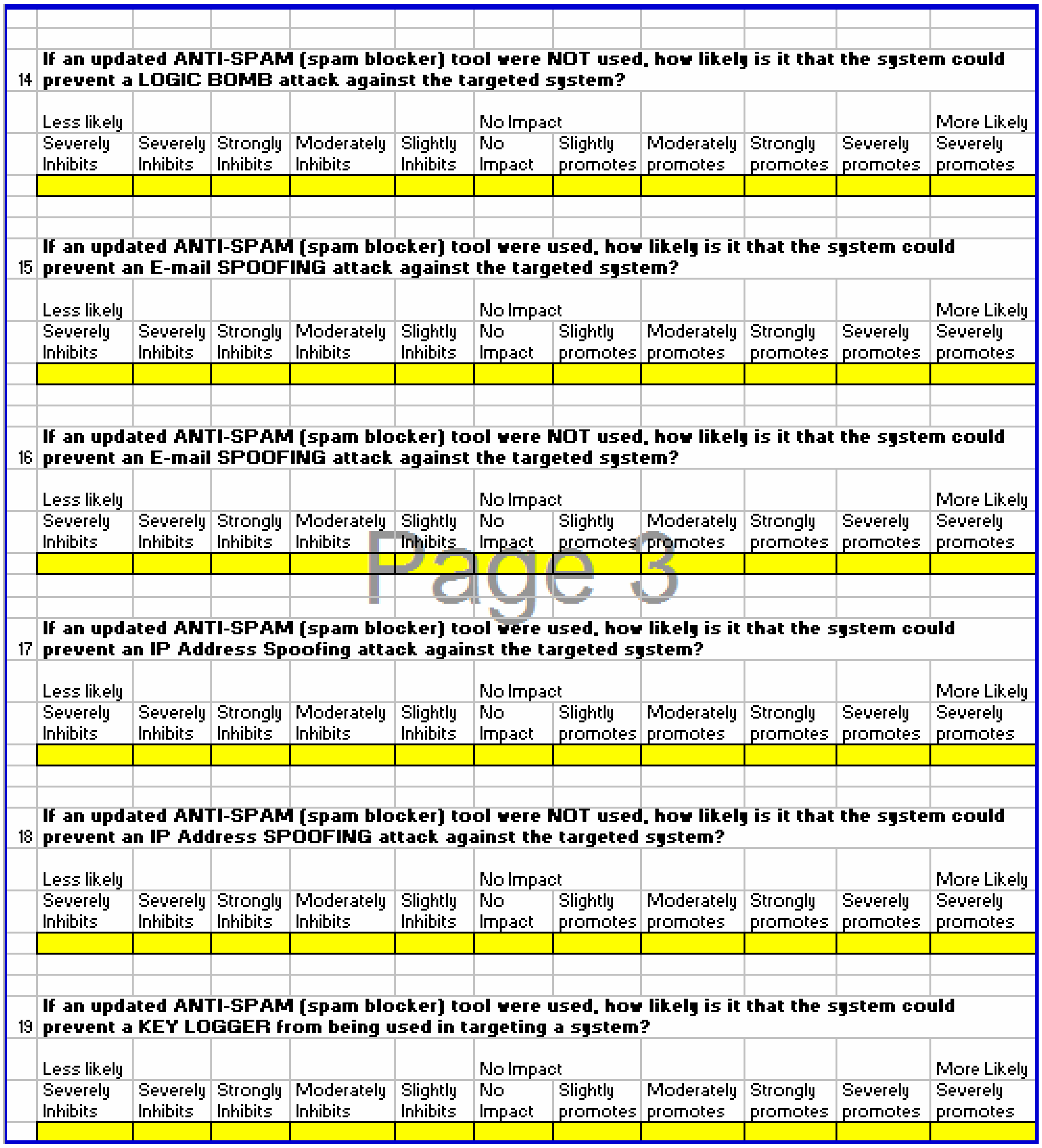
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

12 **If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?**

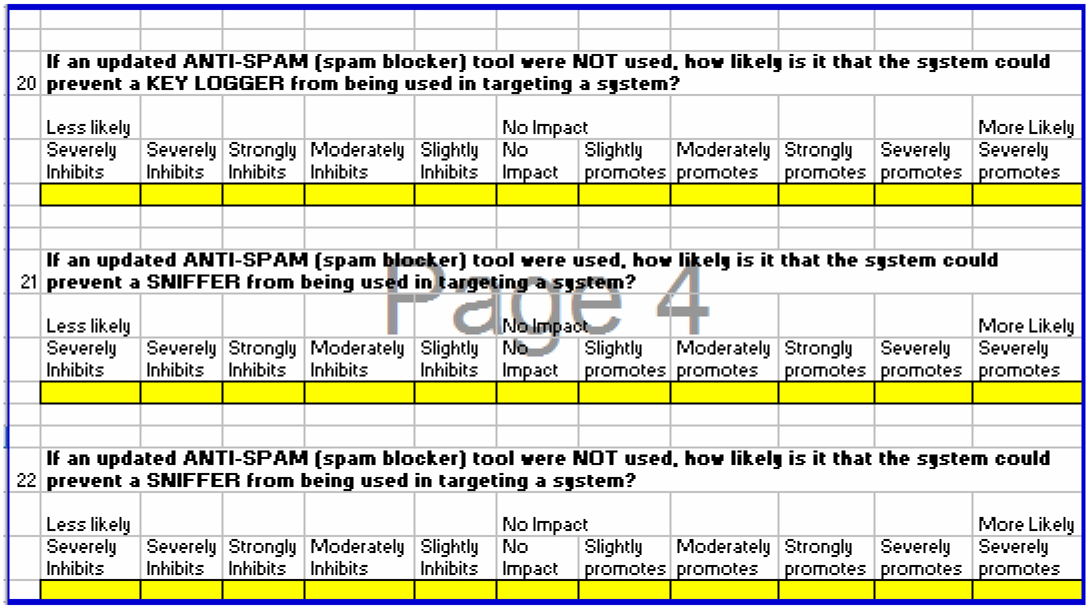
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

13 **If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

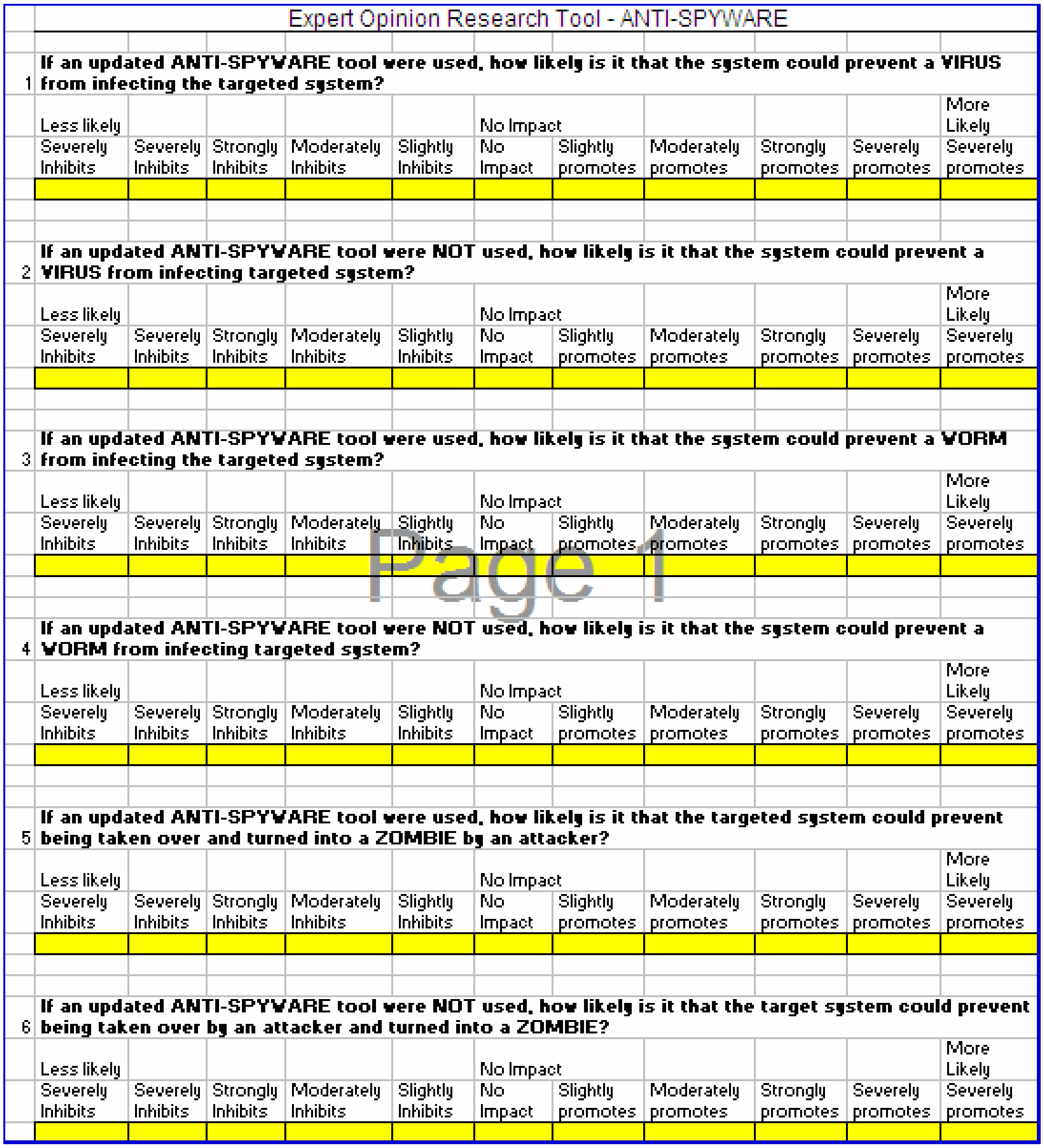


14	If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
15	If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
16	If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
17	If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
18	If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
19	If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



20	**If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
21	**If an updated ANTI-SPAM (spam blocker) tool were used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
22	**If an updated ANTI-SPAM (spam blocker) tool were NOT used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

7. ANTI-SPYWARE SECTION OF SURVEY



Expert Opinion Research Tool - ANTI-SPYWARE

1 If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a VIRUS from infecting the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

2 If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a VIRUS from infecting targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

3 If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a WORM from infecting the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

4 If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a WORM from infecting targeted system?

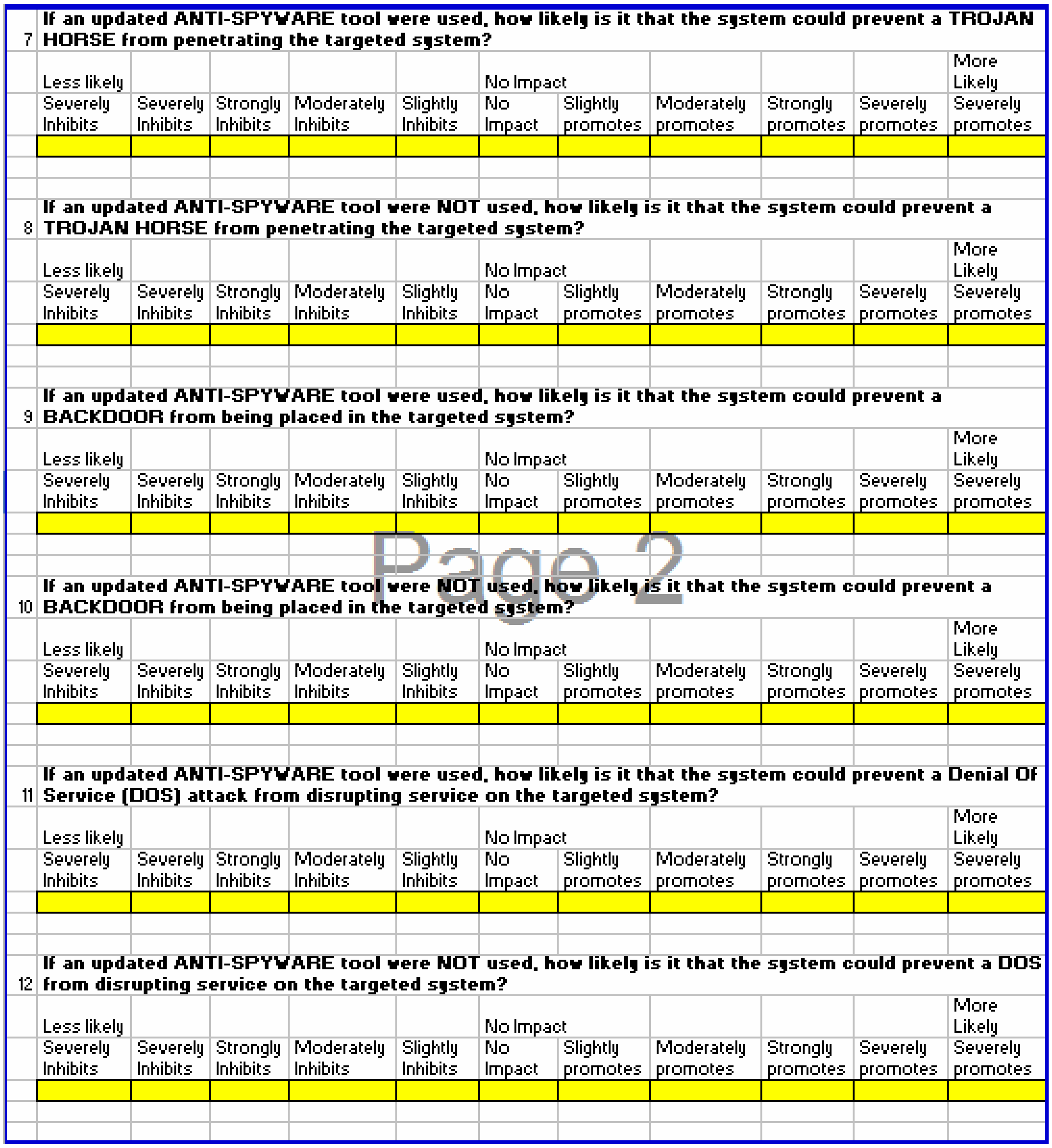
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

5 If an updated ANTI-SPYWARE tool were used, how likely is it that the targeted system could prevent being taken over and turned into a ZOMBIE by an attacker?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

6 If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the target system could prevent being taken over by an attacker and turned into a ZOMBIE?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



7 If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

8 If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a TROJAN HORSE from penetrating the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

9 If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

10 If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a BACKDOOR from being placed in the targeted system?

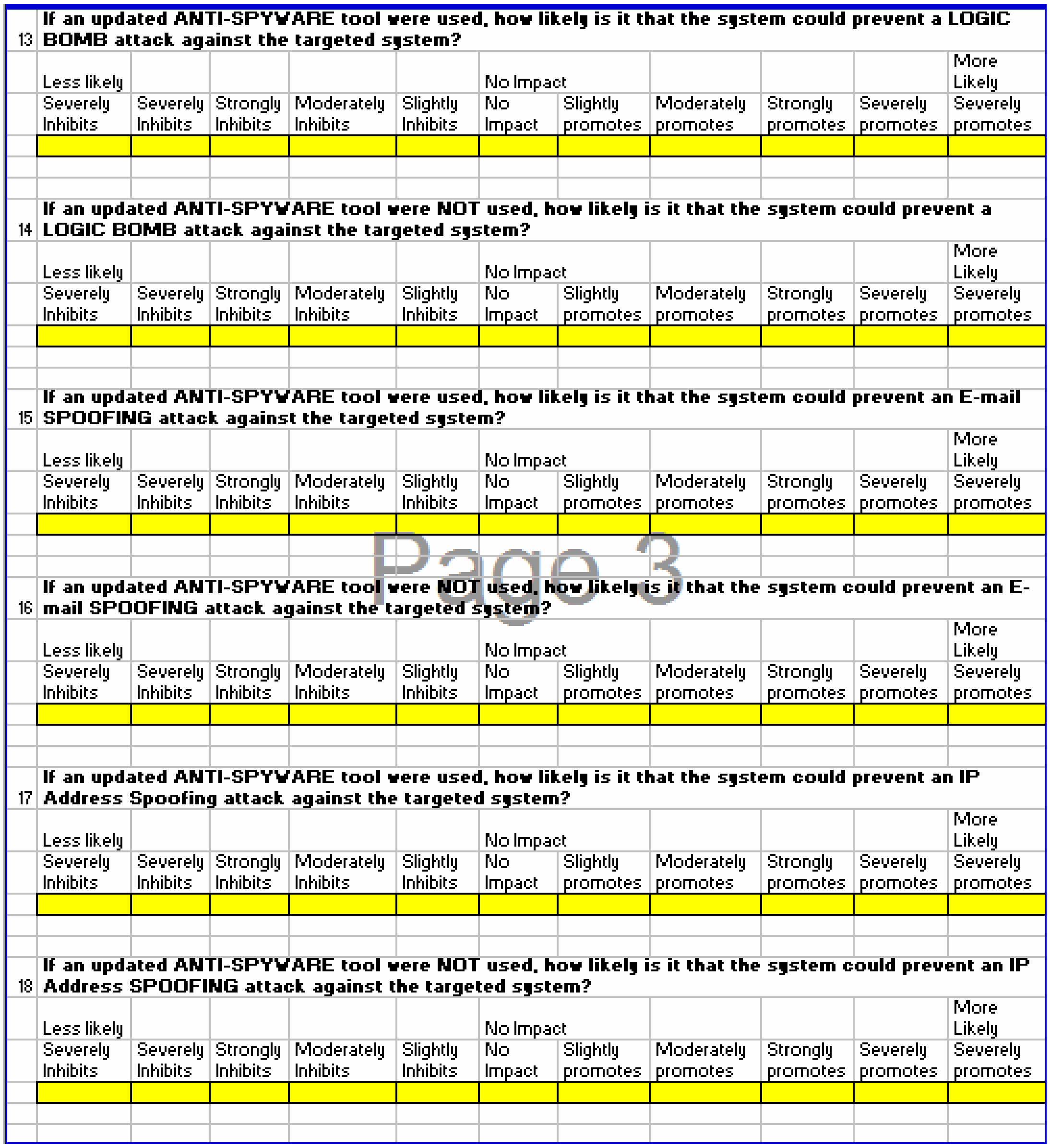
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

11 If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a Denial Of Service (DOS) attack from disrupting service on the targeted system?

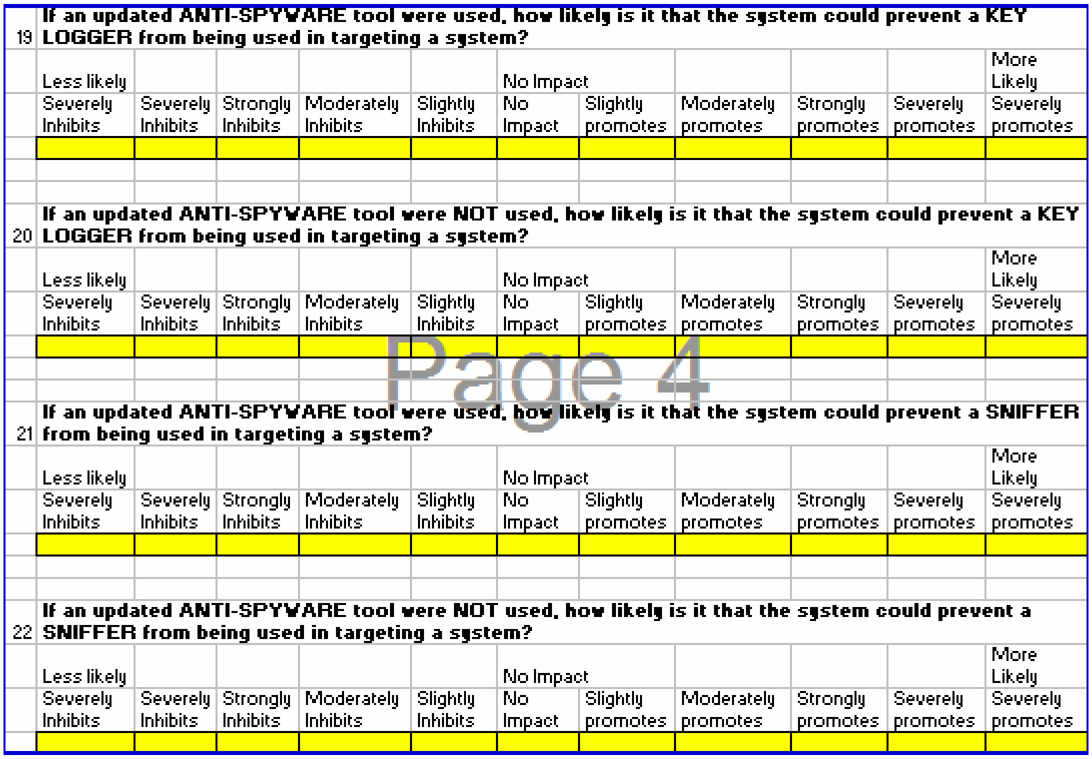
Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

12 If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a DOS from disrupting service on the targeted system?

Less likely					No Impact					More Likely
Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



13	**If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
14	**If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a LOGIC BOMB attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
15	**If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
16	**If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent an E-mail SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
17	**If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent an IP Address Spoofing attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
18	**If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent an IP Address SPOOFING attack against the targeted system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes



19	**If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
20	**If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a KEY LOGGER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
21	**If an updated ANTI-SPYWARE tool were used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes
22	**If an updated ANTI-SPYWARE tool were NOT used, how likely is it that the system could prevent a SNIFFER from being used in targeting a system?**										
	Less likely					No Impact					More Likely
	Severely Inhibits	Severely Inhibits	Strongly Inhibits	Moderately Inhibits	Slightly Inhibits	No Impact	Slightly promotes	Moderately promotes	Strongly promotes	Severely promotes	Severely promotes

THIS PAGE INTENTIONALLY LEFT BLANK

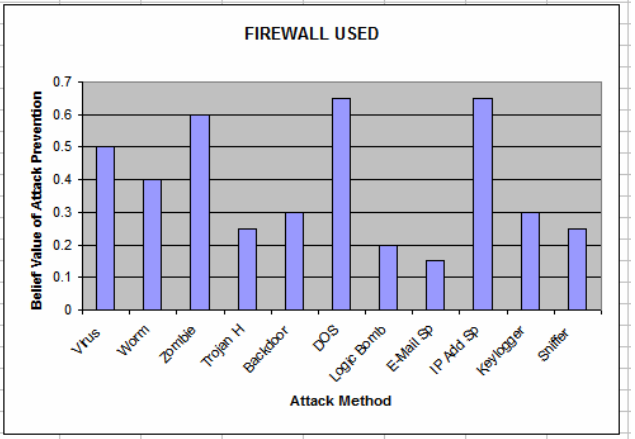
APPENDIX B EXPERT OPINION SUMMARY RESULTS

The following results are comprised from the seven sets of questions which made-up the expert opinion survey. As you may remember from Chapter 2 the survey questions came in pairs. The first question was designed to capture the survey takers judgment of the security measures impact on attack prevention if the measure is employed; the second question was designed to reflect the survey taker's judgment of the impact on not using the security measure. Each question had an eleven category range, spanning from "severely inhibits" to "severely promotes," which matches up with SIAM's measurement techniques for assigning linkage values between nodes. Each of the eleven possible selections has a corresponding numerical value for use in the influence net model, with +1 being severely promoting and a -1 corresponding to severely inhibiting.

1. RESULTS IF FIREWALL WERE USED

	IF PREMISE WERE TRUE				
	Survey1	Survey2	Survey3	Survey4	Average
Firewall					
Virus	0.6	0	1	0.4	0.5
Worm	0.6	0	0.4	0.6	0.4
Zombie	0.6	0.6	0.4	0.8	0.6
Trojan H	0.4	0	0.2	0.4	0.25
Backdoor	0.2	0	0.4	0.6	0.3
DOS	0.8	0.4	0.6	0.8	0.65
Logic Bomb	0.4	0	0	0.4	0.2
E-Mail Sp	0.2	0	0	0.4	0.15
IP Add Sp	0.2	0.8	1	0.6	0.65
Keylogger	0.4	0	0	0.8	0.3
Sniffer	0.4	0	0	0.6	0.25

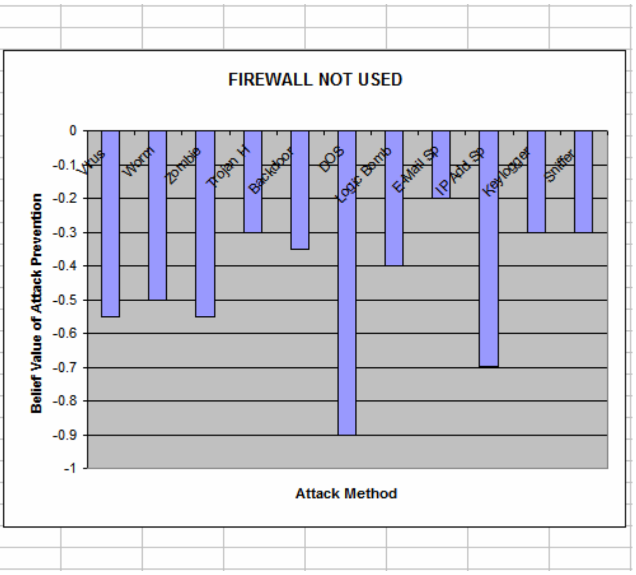
Virus	0.5
Worm	0.4
Zombie	0.6
Trojan H	0.25
Backdoor	0.3
DOS	0.65
Logic Bom	0.2
E-Mail Sp	0.15
IP Add Sp	0.65
Keylogger	0.3
Sniffer	0.25



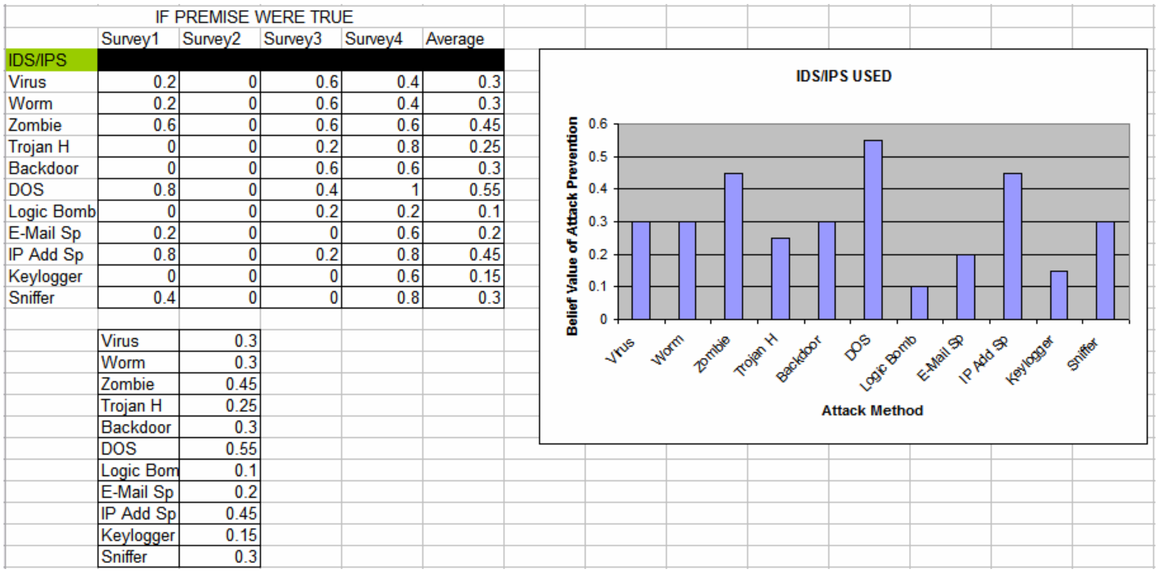
2. RESULTS IF FIREWALL WERE NOT USED

	IF PREMISE WERE FALSE				
	Survey1	Survey2	Survey3	Survey4	Average
Firewall					
Virus	-1	0	-0.6	-0.6	-0.55
Worm	-1	0	-0.4	-0.6	-0.5
Zombie	-0.4	-0.6	-0.4	-0.8	-0.55
Trojan H	-0.4	0	-0.2	-0.6	-0.3
Backdoor	-0.2	0	-0.4	-0.8	-0.35
DOS	-1	-0.6	-1	-1	-0.9
Logic Bomb	-1	0	0	-0.6	-0.4
E-Mail Sp	-0.2	0	0	-0.6	-0.2
IP Add Sp	-0.2	-0.8	-1	-0.8	-0.7
Keylogger	-0.4	0	0	-0.8	-0.3
Sniffer	-0.4	0	0	-0.8	-0.3

Virus	-0.55
Worm	-0.5
Zombie	-0.55
Trojan H	-0.3
Backdoor	-0.35
DOS	-0.9
Logic Bom	-0.4
E-Mail Sp	-0.2
IP Add Sp	-0.7
Keylogger	-0.3
Sniffer	-0.3



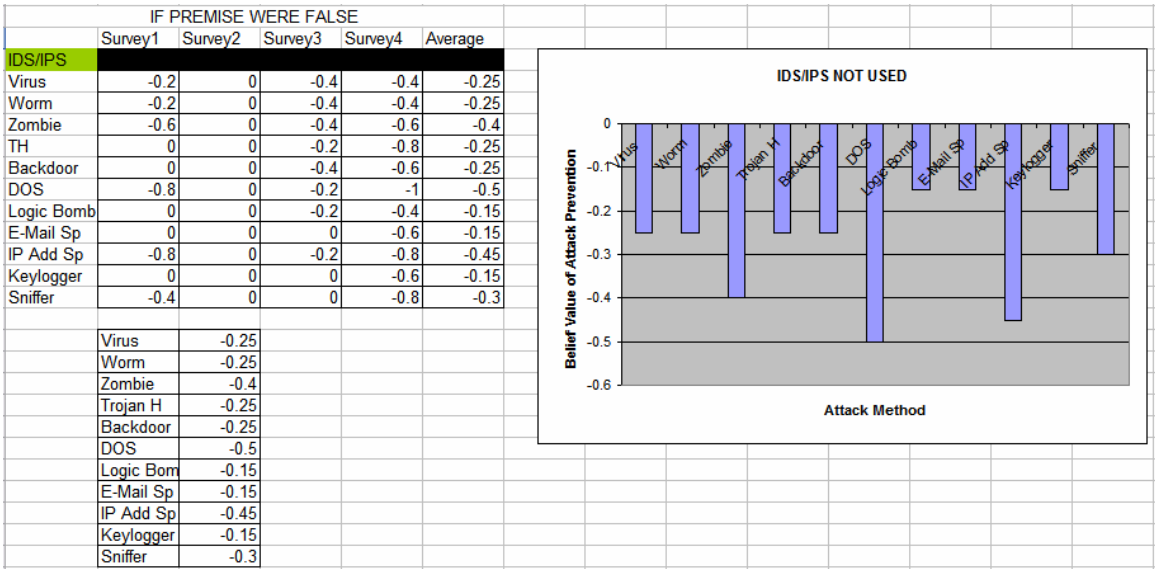
3. RESULTS IF IDS/IPS WERE USED



IF PREMISE WERE TRUE					
	Survey1	Survey2	Survey3	Survey4	Average
IDS/IPS					
Virus	0.2	0	0.6	0.4	0.3
Worm	0.2	0	0.6	0.4	0.3
Zombie	0.6	0	0.6	0.6	0.45
Trojan H	0	0	0.2	0.8	0.25
Backdoor	0	0	0.6	0.6	0.3
DOS	0.8	0	0.4	1	0.55
Logic Bomb	0	0	0.2	0.2	0.1
E-Mail Sp	0.2	0	0	0.6	0.2
IP Add Sp	0.8	0	0.2	0.8	0.45
Keylogger	0	0	0	0.6	0.15
Sniffer	0.4	0	0	0.8	0.3

Virus	0.3
Worm	0.3
Zombie	0.45
Trojan H	0.25
Backdoor	0.3
DOS	0.55
Logic Bom	0.1
E-Mail Sp	0.2
IP Add Sp	0.45
Keylogger	0.15
Sniffer	0.3

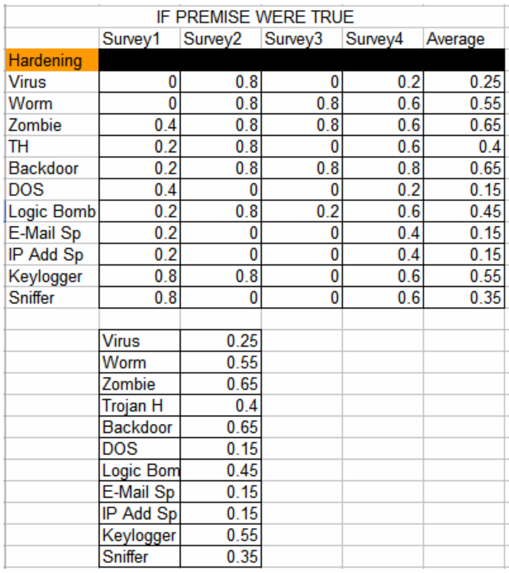
4. RESULTS IF IDS/IPS WERE NOT USED



IF PREMISE WERE FALSE					
	Survey1	Survey2	Survey3	Survey4	Average
IDS/IPS					
Virus	-0.2	0	-0.4	-0.4	-0.25
Worm	-0.2	0	-0.4	-0.4	-0.25
Zombie	-0.6	0	-0.4	-0.6	-0.4
TH	0	0	-0.2	-0.8	-0.25
Backdoor	0	0	-0.4	-0.6	-0.25
DOS	-0.8	0	-0.2	-1	-0.5
Logic Bomb	0	0	-0.2	-0.4	-0.15
E-Mail Sp	0	0	0	-0.6	-0.15
IP Add Sp	-0.8	0	-0.2	-0.8	-0.45
Keylogger	0	0	0	-0.6	-0.15
Sniffer	-0.4	0	0	-0.8	-0.3

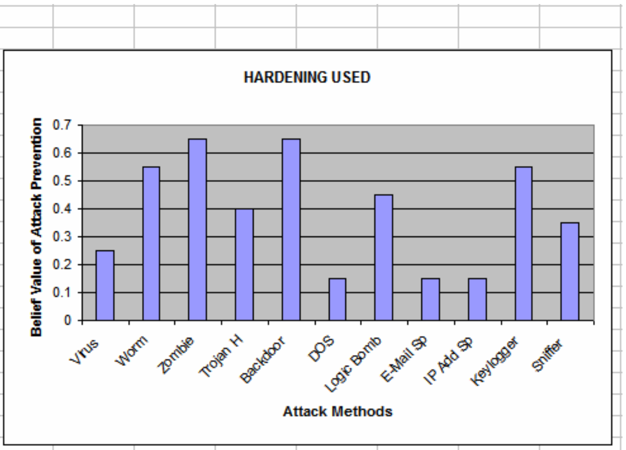
Virus	-0.25
Worm	-0.25
Zombie	-0.4
Trojan H	-0.25
Backdoor	-0.25
DOS	-0.5
Logic Bom	-0.15
E-Mail Sp	-0.15
IP Add Sp	-0.45
Keylogger	-0.15
Sniffer	-0.3

5. RESULTS IF HARDENING WAS USED

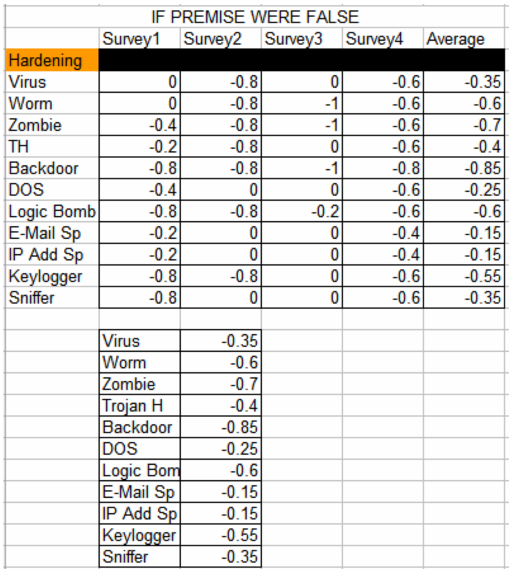


	IF PREMISE WERE TRUE				
	Survey1	Survey2	Survey3	Survey4	Average
Hardening					
Virus	0	0.8	0	0.2	0.25
Worm	0	0.8	0.8	0.6	0.55
Zombie	0.4	0.8	0.8	0.6	0.65
TH	0.2	0.8	0	0.6	0.4
Backdoor	0.2	0.8	0.8	0.8	0.65
DOS	0.4	0	0	0.2	0.15
Logic Bomb	0.2	0.8	0.2	0.6	0.45
E-Mail Sp	0.2	0	0	0.4	0.15
IP Add Sp	0.2	0	0	0.4	0.15
Keylogger	0.8	0.8	0	0.6	0.55
Sniffer	0.8	0	0	0.6	0.35

Virus	0.25
Worm	0.55
Zombie	0.65
Trojan H	0.4
Backdoor	0.65
DOS	0.15
Logic Bom	0.45
E-Mail Sp	0.15
IP Add Sp	0.15
Keylogger	0.55
Sniffer	0.35

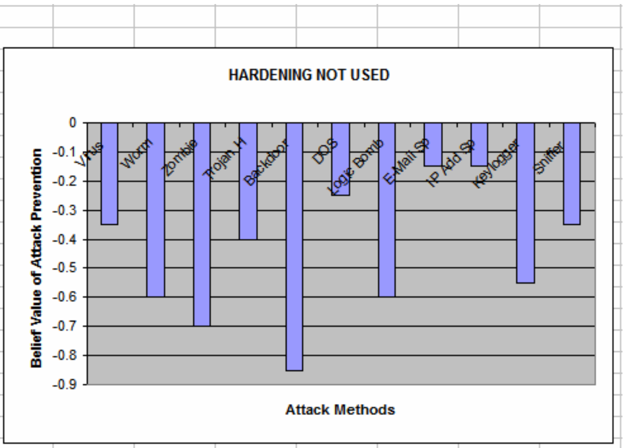


6. RESULTS IF HARDENING WAS NOT USED

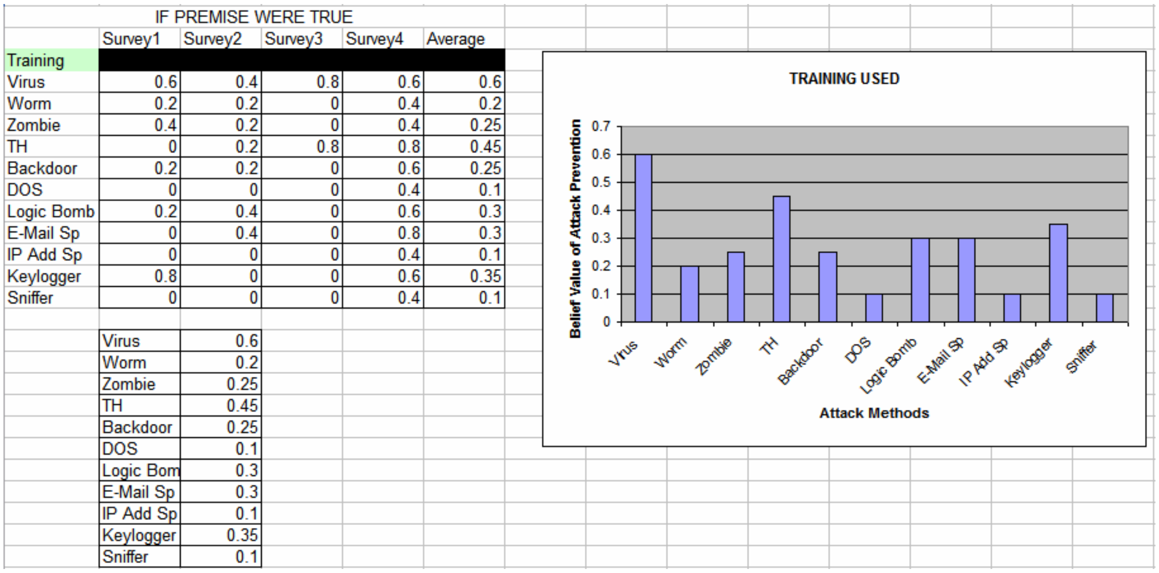


	IF PREMISE WERE FALSE				
	Survey1	Survey2	Survey3	Survey4	Average
Hardening					
Virus	0	-0.8	0	-0.6	-0.35
Worm	0	-0.8	-1	-0.6	-0.6
Zombie	-0.4	-0.8	-1	-0.6	-0.7
TH	-0.2	-0.8	0	-0.6	-0.4
Backdoor	-0.8	-0.8	-1	-0.8	-0.85
DOS	-0.4	0	0	-0.6	-0.25
Logic Bomb	-0.8	-0.8	-0.2	-0.6	-0.6
E-Mail Sp	-0.2	0	0	-0.4	-0.15
IP Add Sp	-0.2	0	0	-0.4	-0.15
Keylogger	-0.8	-0.8	0	-0.6	-0.55
Sniffer	-0.8	0	0	-0.6	-0.35

Virus	-0.35
Worm	-0.6
Zombie	-0.7
Trojan H	-0.4
Backdoor	-0.85
DOS	-0.25
Logic Bom	-0.6
E-Mail Sp	-0.15
IP Add Sp	-0.15
Keylogger	-0.55
Sniffer	-0.35



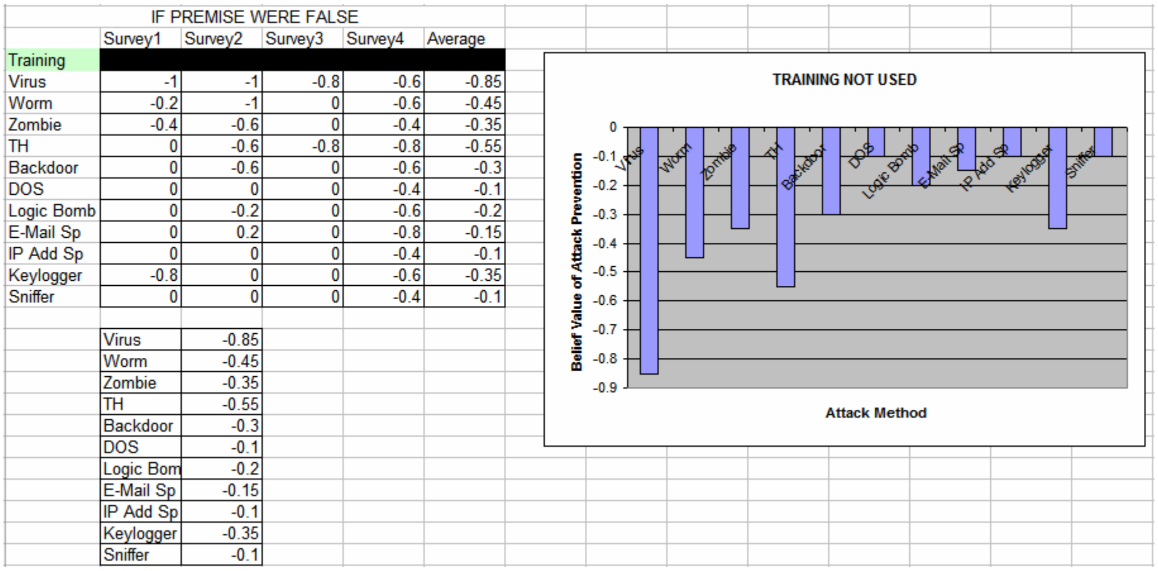
7. RESULTS IF ADEQUATE TRAINING WAS USED



	IF PREMISE WERE TRUE				
	Survey1	Survey2	Survey3	Survey4	Average
Training					
Virus	0.6	0.4	0.8	0.6	0.6
Worm	0.2	0.2	0	0.4	0.2
Zombie	0.4	0.2	0	0.4	0.25
TH	0	0.2	0.8	0.8	0.45
Backdoor	0.2	0.2	0	0.6	0.25
DOS	0	0	0	0.4	0.1
Logic Bomb	0.2	0.4	0	0.6	0.3
E-Mail Sp	0	0.4	0	0.8	0.3
IP Add Sp	0	0	0	0.4	0.1
Keylogger	0.8	0	0	0.6	0.35
Sniffer	0	0	0	0.4	0.1

Virus	0.6
Worm	0.2
Zombie	0.25
TH	0.45
Backdoor	0.25
DOS	0.1
Logic Bom	0.3
E-Mail Sp	0.3
IP Add Sp	0.1
Keylogger	0.35
Sniffer	0.1

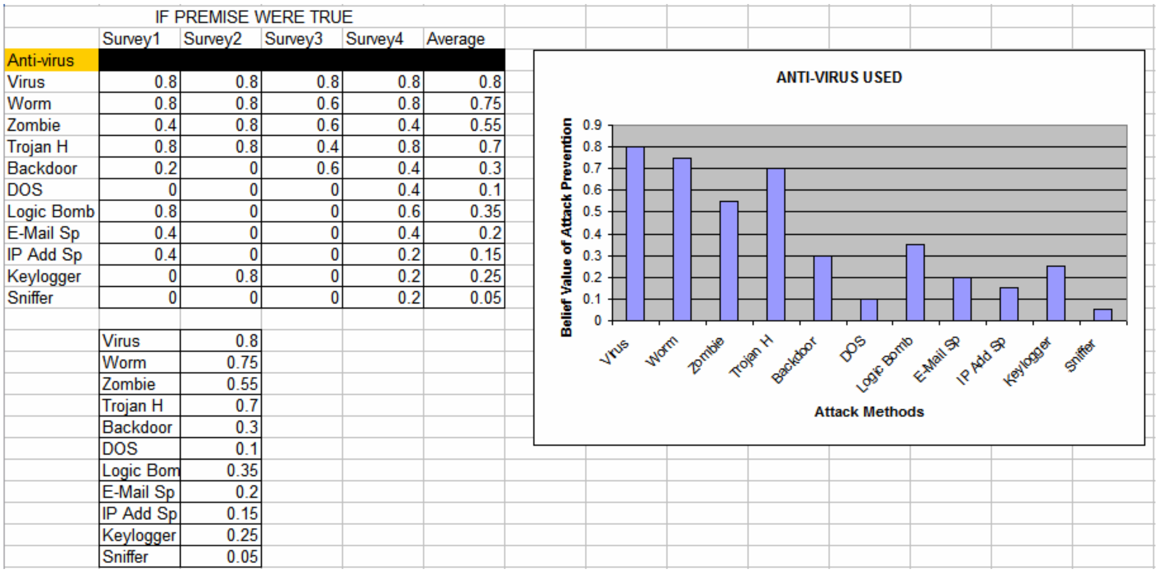
8. RESULTS IF ADEQUATE TRAINING WERE NOT USED



	IF PREMISE WERE FALSE				
	Survey1	Survey2	Survey3	Survey4	Average
Training					
Virus	-1	-1	-0.8	-0.6	-0.85
Worm	-0.2	-1	0	-0.6	-0.45
Zombie	-0.4	-0.6	0	-0.4	-0.35
TH	0	-0.6	-0.8	-0.8	-0.55
Backdoor	0	-0.6	0	-0.6	-0.3
DOS	0	0	0	-0.4	-0.1
Logic Bomb	0	-0.2	0	-0.6	-0.2
E-Mail Sp	0	0.2	0	-0.8	-0.15
IP Add Sp	0	0	0	-0.4	-0.1
Keylogger	-0.8	0	0	-0.6	-0.35
Sniffer	0	0	0	-0.4	-0.1

Virus	-0.85
Worm	-0.45
Zombie	-0.35
TH	-0.55
Backdoor	-0.3
DOS	-0.1
Logic Bom	-0.2
E-Mail Sp	-0.15
IP Add Sp	-0.1
Keylogger	-0.35
Sniffer	-0.1

9. RESULTS IF ANTI-VIRUS SOFTWARE WAS USED

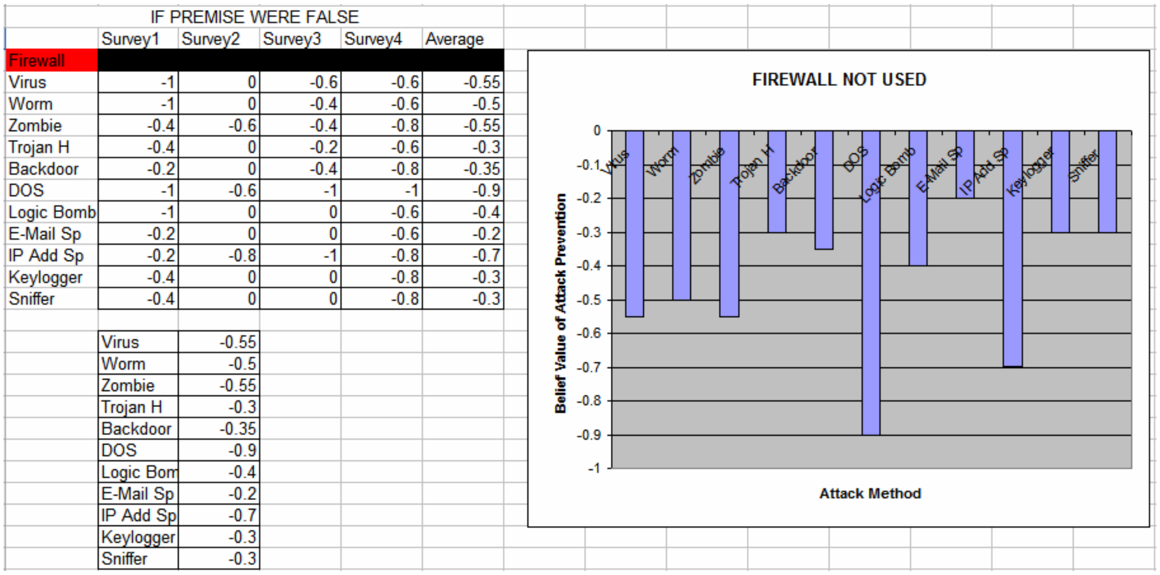


IF PREMISE WERE TRUE

	Survey1	Survey2	Survey3	Survey4	Average
Anti-virus					
Virus	0.8	0.8	0.8	0.8	0.8
Worm	0.8	0.8	0.6	0.8	0.75
Zombie	0.4	0.8	0.6	0.4	0.55
Trojan H	0.8	0.8	0.4	0.8	0.7
Backdoor	0.2	0	0.6	0.4	0.3
DOS	0	0	0	0.4	0.1
Logic Bomb	0.8	0	0	0.6	0.35
E-Mail Sp	0.4	0	0	0.4	0.2
IP Add Sp	0.4	0	0	0.2	0.15
Keylogger	0	0.8	0	0.2	0.25
Sniffer	0	0	0	0.2	0.05

Virus	0.8
Worm	0.75
Zombie	0.55
Trojan H	0.7
Backdoor	0.3
DOS	0.1
Logic Bom	0.35
E-Mail Sp	0.2
IP Add Sp	0.15
Keylogger	0.25
Sniffer	0.05

10. RESULTS IF ANTI-VIRUS SOFTWARE WAS NOT USED

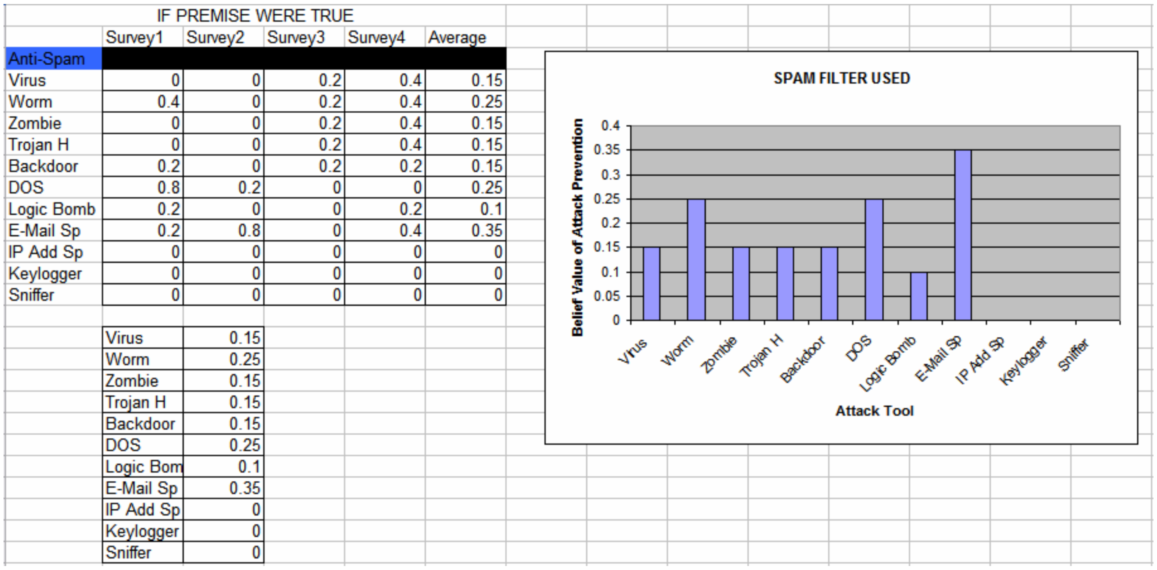


IF PREMISE WERE FALSE

	Survey1	Survey2	Survey3	Survey4	Average
Firewall					
Virus	-1	0	-0.6	-0.6	-0.55
Worm	-1	0	-0.4	-0.6	-0.5
Zombie	-0.4	-0.6	-0.4	-0.8	-0.55
Trojan H	-0.4	0	-0.2	-0.6	-0.3
Backdoor	-0.2	0	-0.4	-0.8	-0.35
DOS	-1	-0.6	-1	-1	-0.9
Logic Bomb	-1	0	0	-0.6	-0.4
E-Mail Sp	-0.2	0	0	-0.6	-0.2
IP Add Sp	-0.2	-0.8	-1	-0.8	-0.7
Keylogger	-0.4	0	0	-0.8	-0.3
Sniffer	-0.4	0	0	-0.8	-0.3

Virus	-0.55
Worm	-0.5
Zombie	-0.55
Trojan H	-0.3
Backdoor	-0.35
DOS	-0.9
Logic Bom	-0.4
E-Mail Sp	-0.2
IP Add Sp	-0.7
Keylogger	-0.3
Sniffer	-0.3

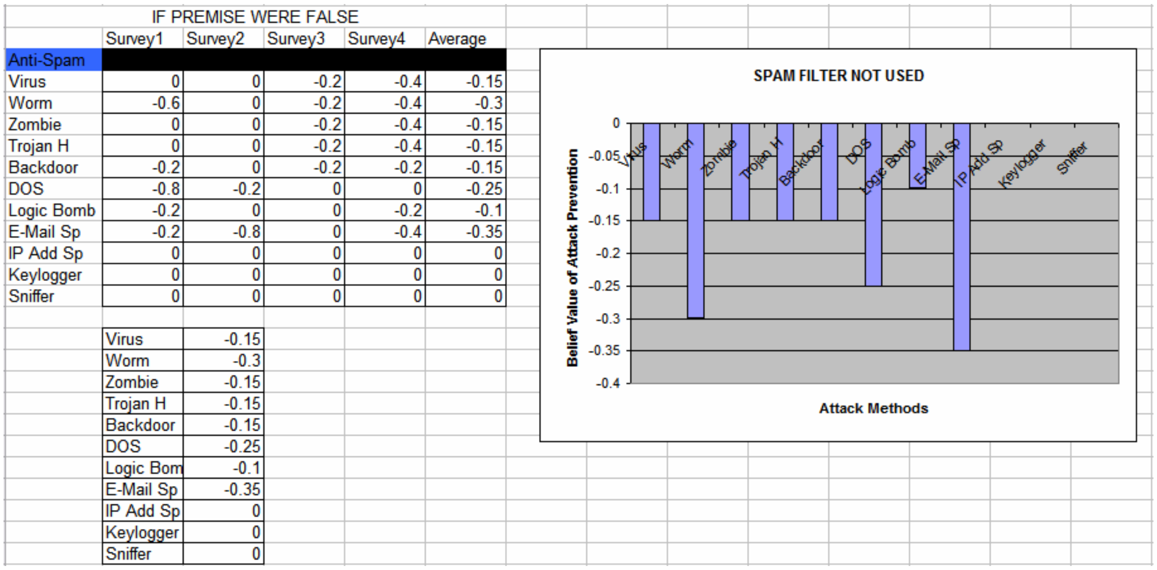
11. RESULTS IF SPAM FILTER WERE USED



	IF PREMISE WERE TRUE				
	Survey1	Survey2	Survey3	Survey4	Average
Anti-Spam					
Virus	0	0	0.2	0.4	0.15
Worm	0.4	0	0.2	0.4	0.25
Zombie	0	0	0.2	0.4	0.15
Trojan H	0	0	0.2	0.4	0.15
Backdoor	0.2	0	0.2	0.2	0.15
DOS	0.8	0.2	0	0	0.25
Logic Bomb	0.2	0	0	0.2	0.1
E-Mail Sp	0.2	0.8	0	0.4	0.35
IP Add Sp	0	0	0	0	0
Keylogger	0	0	0	0	0
Sniffer	0	0	0	0	0

Virus	0.15
Worm	0.25
Zombie	0.15
Trojan H	0.15
Backdoor	0.15
DOS	0.25
Logic Bom	0.1
E-Mail Sp	0.35
IP Add Sp	0
Keylogger	0
Sniffer	0

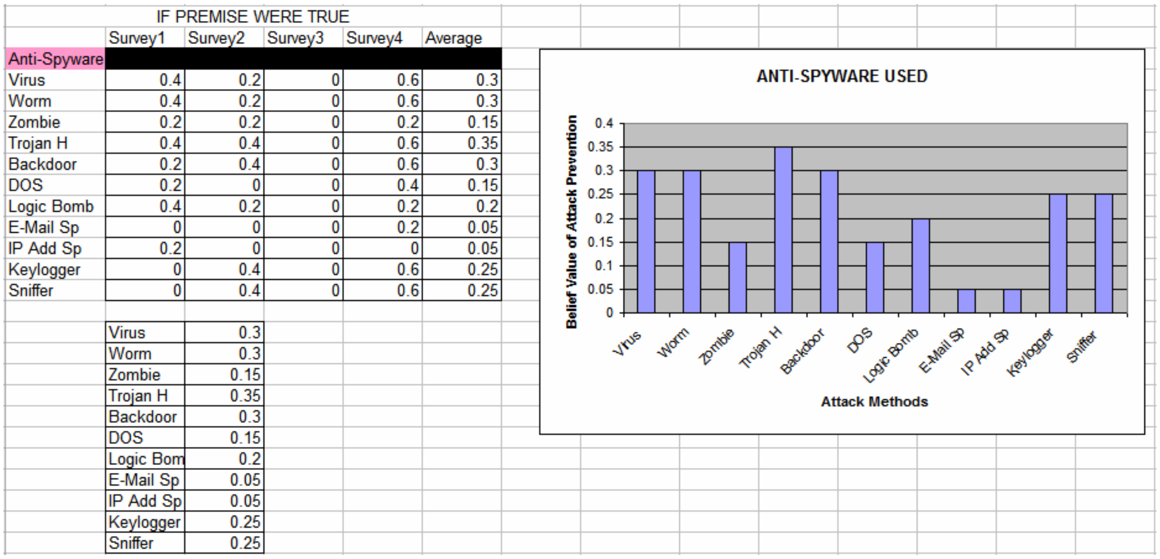
12. RESULTS IF SPAM FILTER WERE NOT USED



	IF PREMISE WERE FALSE				
	Survey1	Survey2	Survey3	Survey4	Average
Anti-Spam					
Virus	0	0	-0.2	-0.4	-0.15
Worm	-0.6	0	-0.2	-0.4	-0.3
Zombie	0	0	-0.2	-0.4	-0.15
Trojan H	0	0	-0.2	-0.4	-0.15
Backdoor	-0.2	0	-0.2	-0.2	-0.15
DOS	-0.8	-0.2	0	0	-0.25
Logic Bomb	-0.2	0	0	-0.2	-0.1
E-Mail Sp	-0.2	-0.8	0	-0.4	-0.35
IP Add Sp	0	0	0	0	0
Keylogger	0	0	0	0	0
Sniffer	0	0	0	0	0

Virus	-0.15
Worm	-0.3
Zombie	-0.15
Trojan H	-0.15
Backdoor	-0.15
DOS	-0.25
Logic Bom	-0.1
E-Mail Sp	-0.35
IP Add Sp	0
Keylogger	0
Sniffer	0

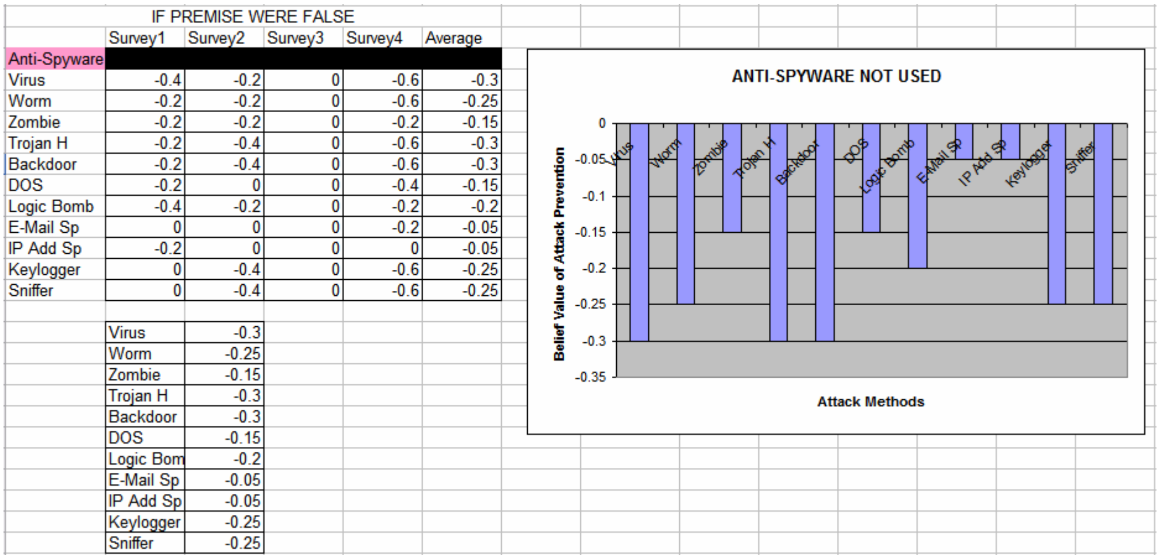
13. RESULTS IF ANTI-SPYWARE WERE USED



	IF PREMISE WERE TRUE				
	Survey1	Survey2	Survey3	Survey4	Average
Anti-Spyware					
Virus	0.4	0.2	0	0.6	0.3
Worm	0.4	0.2	0	0.6	0.3
Zombie	0.2	0.2	0	0.2	0.15
Trojan H	0.4	0.4	0	0.6	0.35
Backdoor	0.2	0.4	0	0.6	0.3
DOS	0.2	0	0	0.4	0.15
Logic Bomb	0.4	0.2	0	0.2	0.2
E-Mail Sp	0	0	0	0.2	0.05
IP Add Sp	0.2	0	0	0	0.05
Keylogger	0	0.4	0	0.6	0.25
Sniffer	0	0.4	0	0.6	0.25

Virus	0.3
Worm	0.3
Zombie	0.15
Trojan H	0.35
Backdoor	0.3
DOS	0.15
Logic Bom	0.2
E-Mail Sp	0.05
IP Add Sp	0.05
Keylogger	0.25
Sniffer	0.25

14. RESULTS IF ANTI-SPYWARE WERE NOT USED



	IF PREMISE WERE FALSE				
	Survey1	Survey2	Survey3	Survey4	Average
Anti-Spyware					
Virus	-0.4	-0.2	0	-0.6	-0.3
Worm	-0.2	-0.2	0	-0.6	-0.25
Zombie	-0.2	-0.2	0	-0.2	-0.15
Trojan H	-0.2	-0.4	0	-0.6	-0.3
Backdoor	-0.2	-0.4	0	-0.6	-0.3
DOS	-0.2	0	0	-0.4	-0.15
Logic Bomb	-0.4	-0.2	0	-0.2	-0.2
E-Mail Sp	0	0	0	-0.2	-0.05
IP Add Sp	-0.2	0	0	0	-0.05
Keylogger	0	-0.4	0	-0.6	-0.25
Sniffer	0	-0.4	0	-0.6	-0.25

Virus	-0.3
Worm	-0.25
Zombie	-0.15
Trojan H	-0.3
Backdoor	-0.3
DOS	-0.15
Logic Bom	-0.2
E-Mail Sp	-0.05
IP Add Sp	-0.05
Keylogger	-0.25
Sniffer	-0.25

LIST OF REFERENCES

Adams, James. The Next World War: Computers are the Weapons & the Front Line is Everywhere. New York: Simon and Schuster, 1998.

Arquilla, John. Interview with FRONTLINE. Cyberwar!: FRONTLINE. 4 Mar. 2003. 8 Mar. 2007 <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/arquilla.html>.

Billo, Charles G., and Welton Chang. Cyber Warfare: an Analysis of the Means and Motivations of Selected Nation States. Institute for Security Technology Studies, Dartmouth College. Hanover: Trustees of Dartmouth College, 2004.

Brodhun III, Carl P. Prioritization of Information Assurance (IA) Technology in a Resource Constrained Environment. Thesis. Naval Postgraduate School, 2001. Monterey: Naval Postgraduate School, 2001.

Cragin, Kim, and Sara A. Daly. The Dynamic Terrorist Threat: an Assessment of Group Motivations and Capabilities in a Changing World. RAND Corporation. Santa Monica: RAND Corporation, 2004.

Denning, Dorothy E. Cyberterrorism: Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, Washington. D.C. 23 May 2000. 8 Mar. 2007 <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

Denning, Dorothy E. Information Warfare and Security. New York: Addison-Wesley, 1999.

Denning, Dorothy E. Is Cyber Terror Next. Social Science Research Council. Georgetown: Social Science Research Council / After Sept 11. 8 Mar. 2007 <http://www.ssrc.org/sept11/essays/denning_text_only.html>.

Gross, Grant. "U.S. DHS Completes Large-Scale Cyber Exercise: Cyber Storm Simulates Attack on Computer Systems At an Electric Utility, Cybersecurity Vendors Kick of Analysis of Results." InfoWorld (2006). 8 Mar. 2007.

"IBM Report: Government, Financial Services and Manufacturing Sectors Top Targets of Security Attacks in First Half of 2005." IBM News. 4 Aug. 2005. 22 Feb. 2007 <http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html>.

Janczewski, Lech J., and Andrew M. Colarik. Managerial Guide for Handling Cyber-Terrorism and Information Warfare. Hershey: Idea Group, 2005.

Lemos, Robert. "Safety: Assessing the Infrastructure Risk." CNET News. 26 Aug. 2006. 8 Mar. 2007 <http://news.com.com/2009-1001-954780.html>.

Lewis, Ted G. Critical Infrastructure Protection in Homeland Security: Defending a Networked System. New Jersey: John Wiley & Sons Inc., 2006.

Libicki, Martin C. "Information Dominance." Strategic Forum (1997). 8 Mar. 2007 <http://www.ndu.edu/inss/strforum/SF132/forum132.html>.

Peltier, Thomas R. Information Security Risk Analysis. Second ed. Boca Raton: Auerbach Publications, 2005.

Rollins, John, and Clay Wilson. Terrorist Capabilities for Cyberattack: Overview and Policy Issues. CRS Report for Congress. Washington, D.C.: Congressional Research Service - the Library of Congress, 2005.

Rosen, Julie A., and Wayne L. Smith. Situational Influence Assessment Module (SIAM) User's Manual. 6th ed. San Diego: Science Applications International Corporation, 2006.

Sands, Jeffrey I., and Bradd C. Hayes, comps. Understanding and Using SIAM. Naval War College, Center for Naval Warfare Studies, Decision Support Department. 15 Jan. 2007 <http://www.au.af.mil/au/awc/awcgate/modeling/usesiam.doc>.

"SANS Top 20-Internet Security Attack Targets." SANS. 8 Mar. 2007. Escal Institute of Advanced Technologies. 8 Mar. 2007 <http://www.sans.org/top20/>.

Serabian Jr., John A. "Cyber Threats and the U.S. Economy." Joint Economic Committee. Washington. D.C. 23 Feb. 2000. 8 Mar. 2007 <http://www.cia.gov/cia/public_affairs/speeches/2000/cyberthreats_022300.html>.

Thomas, Douglas, and Brian D. Loader. Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. New York: Routledge, 2000.

United States. Assistant Secretary of Defense for Command, Control, Communications and Intelligence. Department of Defense. DoD Directive 8500.1 Information Assurance (IA). Washington D.C.: DoD, 2002.

United States. Chairman. Joint Chiefs of Staff. Joint Publication 3-13 Information Operations. Washington D.C.: Joint Chiefs of Staff, 2006.

United States. Department of Defense. DoD Directive 8500.2 Information Assurance (IA) Implementation. Washington D.C.: DoD, 2003.

United States. National Manager, Committee on National Security Systems (CNSS). National Security Agency. CNSS Instruction No. 4009 National Information Assurance (IA) Glossary. Washington D.C.: CNSS, 2003.

United States. President of the United States. The National Strategy to Secure Cyberspace. Washington D.C.: The White House, 2003.

Wilson, Clay. Information Warfare and Cyberwar: Capabilities and Related Policy Issues. CRS Report for Congress. Washington, D.C.: Congressional Research Service - the Library of Congress, 2004.

Woody, Carol, and Larry Clinton. Common Sense Guide to Cyber Security for Small Businesses. 1st ed. Arlington: Carnegie Mellon University and Internet Security Alliance, 2004. Recommended Actions for Information Security. 8 Mar. 2007 <http://www.us-cert.gov/reading_room/CSG-small-business.pdf>.

Verton, Dan. Black Ice: the Invisible Threat of Cyber-Terrorism. New York: McGraw-Hill/Osborne, 2003.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Dan C. Boger
   Naval Postgraduate School
   Monterey, California

4. Dr. Dorothy E. Denning
   Naval Postgraduate School
   Monterey, California

5. Mr. Steve Iatrou
   Naval Postgraduate School
   Monterey, California